Titre: Title:	Mécanisme FH-RSVP pour la relève intrasite dans les réseaux hiérarchiques mobile IPV6
Auteur: Author:	Stéphane Fobah Elleingand
Date:	2004
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Elleingand, S. F. (2004). Mécanisme FH-RSVP pour la relève intrasite dans les réseaux hiérarchiques mobile IPV6 [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7374/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/7374/
Directeurs de recherche: Advisors:	
Programme: Program:	Non spécifié

UNIVERSITÉ DE MONTRÉAL

MÉCANISME FH-RSVP POUR LA RELÈVE INTRASITE DANS LES RÉSEAUX HIÉRARCHIQUES MOBILE IPV6

STÉPHANE FOBAH ELLEINGAND
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)

DÉCEMBRE 2004

Your file Votre référence
ISBN: 0-494-01319-2
Our file Notre référence
ISBN: 0-494-01319-2

UNIVERSITÉ DE MONTRÉAL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

MÉCANISME FH-RSVP POUR LA RELÈVE INTRASITE
DANS LES RÉSEAUX HIÉRARCHIQUES MOBILE IPV6

présenté par : ELLEINGAND Stéphane Fobah
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

M. ROY Robert, Ph.D, président
M. PIERRE Samuel, Ph.D, membre, directeur de recherche
M. QUINTERO Alejandro, Doct., membre

DÉDICACE

Je voudrais tout d'abord dédier ce mémoire à mes parents et les remercier pour tous les sacrifices qu'ils ont faits pour moi.

Madame Améthier Jeanne Taki, chère Maman, je voulais te dire mille et une fois merci pour TOUT.

Monsieur Elleingand Etché Alexis, cher Père, je voulais te dire mille et une fois merci pour TOUT.

Je voulais également remercier Monsieur Améthier Jean-Baptiste. Cher Grand-Père, tu as toujours été une source d'inspiration profonde à tous les niveaux.

REMERCIEMENTS

Je voudrais tout d'abord remercier mon directeur de recherche M. Samuel Pierre pour avoir cru que je pouvais mener à bien ce travail et pour son apport scientifique.

Je tiens à remercier mon ami Charles Martial Abondo pour sa contribution intellectuelle et nos longues discussions, mes collègues du Laboratoire de Recherche en Réseautique et Informatique Mobile (LARIM) pour leurs critiques et leurs conseils. Merci tout spécialement à Larbi Alaoui Belhriti, Jihad Hodroj, Mamadou M. Diallo, Christiane F. Dzongang.

Merci à mes frères et sœurs, Marie-Laure, Patrice, Franck et Aniéla, ainsi qu'à mes cousins et amis pour leur soutien permanent et leurs encouragements.

RÉSUMÉ

Au cours des dernières années, le monde des communications sans fil a connu des changements qui ont créé un immense besoin en garantie de qualité de service (QdS). Le protocole Mobile IP apparaît comme l'un des protocoles les plus prometteurs de l'Internet mobile de prochaine génération. Bien que RSVP soit un protocole mature de réservation de ressources réseau, lorsqu'il est utilisé dans des environnements mobiles ayant Mobile IP comme protocole de gestion de mobilité, de nombreux problèmes surviennent en terme de détérioration de la qualité de service parce que RSVP a été conçu à l'origine pour des environnement fixes (i.e. avec des hôtes et postes fixes). Un usager mobile qui se retrouve à l'intérieur d'une zone fait des requêtes de service au réseau; par conséquent, le réseau a besoin d'offrir une certaine garantie sur la qualité de service de ces requêtes. Si, en cours de communication, un usager mobile se déplace d'un réseau d'accès à un autre, il s'agit alors de pouvoir établir la qualité de service le long du nouveau chemin de communication. Ceci constitue le problème de l'impact de la mobilité d'un hôte mobile sur la qualité de service.

L'objectif de ce mémoire est de proposer une solution de QdS permettant de garantir la réservation de ressources pour des applications temps réel échangées entre un nœud mobile dont le medium radio est le *WLAN* et son nœud correspondant, en tenant compte du processus de relève intra-site du nœud mobile. Notre but est de développer un mécanisme de QdS rapide, efficace et peu glouton en terme de consommation de ressources.

Étant donné que la mobilité d'un usager est essentiellement de la mobilité régionale, nous avons choisi de bâtir notre mécanisme sur une architecture *Hierarchical Mobile IPv6* et de consacrer nos efforts sur la relève intra-domaine MAP. Nous avons donc privilégié la méthode de réservation par anticipation en combinaison avec une variante du protocole RSVP, dit orienté émetteur, contrairement à la première version de RSVP qui est orientée récepteur. L'anticipation de la réservation utilise le principe de la *relève rapide* pour réserver des ressources dès qu'une relève est détectée par FMIPv6.

Nous avons implémenté deux versions de la méthode proposée et nous avons fait des séries d'expériences pour analyser la performance, en mettant l'accent dans un premier temps sur le délai de mise à jour de la QdS (DMQ), le débit de l'application au nœud MN, la latence de la relève et la perte de paquet. Nous avons étudié l'effet de la vitesse du nœud mobile MN, du débit de l'application et du délai de transmission de l'Internet. Puis, dans un deuxième temps, nous avons évaluer, également, FH-RSVP en terme de probabilités de blocage d'une réservation, d'interruption forcée d'une réservation et de compléter avec succès une session. Nous avons étudié l'impact de la charge totale offerte, du pourcentage total de MNs provenant de cellules adjacentes qui font une *relève* vers la cellule courante et de la vitesse du nœud MN.

Pour évaluer la performance de FH-RSVP, nous avons comparé nos résultats à ceux obtenus avec le protocole MRSVP. En général, nous remarquons que le nombre de paquets rejetés, la latence de la relève avec MRSVP est toujours plus grand que celui avec FH-RSVP. Lorsque le délai DMQ est évalué par rapport aux réservations passives, il est évident que MRSVP sera plus rapide que FH-RSVP puisque MRSVP réserve passivement des ressources avant même le déclenchement d'une relève. Par contre, le délai moyen DMQ du protocole MRSVP pour activer les ressources passives dans la nouvelle cellule est toujours plus élevé que celui du FH-RSVP. Ces résultats sur la perte de paquets, la latence de la relève, le débit de l'application étaient prévisibles car MRSVP utilise pour la gestion de la mobilité un module Mobile IPv4 qui ne comprend pas les protocoles complémentaires *Hierarchical Mobile IPv6* et *Fast Mobile IPv6*. En utilisant *Fast Mobile IPv6* et *Hierarchical Mobile IPv6*, dans FH-RSVP, nous réduisons le temps de latence et implicitement la perte de paquets. Les résultats sur les probabilités de blocage d'une réservation, d'interruption forcée d'une réservation et de compléter avec succès une session étaient prévisibles dans la mesure où le protocole MRSVP fait un gaspillage des ressources en réservant excessivement des ressources passives à l'intérieur des cellules voisines de la cellule courante où se trouve le nœud mobile.

ABSTRACT

During the past years, several researches have been made to develop functionality for mobility management support and QoS provision in all-IP networks. Since IP was not designed to support such functionality, new protocols such as Mobile IP have been specified and implemented to resolve these issues. Mobile IP is currently one of the most important protocols for next generation mobile Internet that allows users to maintain connectivity while roaming in IP networks. Mobile IPv6 (MIPv6) provides many features such as sufficient address space, mobility, security and QoS. RSVP is a well mature protocol for reserving network resources to support QoS requirements between sender and receiver(s). RSVP was originally developed for fixed networks and when combined in mobile environments using Mobile IP as the mobility management protocol several issues arise in terms of QoS deterioration.

To reduce these inefficiencies, our objective is to propose a new RSVP extension sender oriented to support real-time service in Hierarchical Mobile IPv6 environments with Fast Handovers (Fast Mobile IPv6). Our scheme integrates RSVP based sender oriented with Mobile IP regional registration and Fast Handover principles and makes advance resources reservation when an intra-site handoff may possibly occur.

We developed a method called FH-RSVP (Fast handover and Hierarchical mobile IPv6 RSVP). We implemented two versions of that method. For the performance analysis, we made several tests, and we compare our results with those of MRSVP protocol. We focused first on the time to establish the new path of quality of service, the application throughput, the *handover* latency and the packet loss. We also evaluated reservation blocking, forced termination, session completion probabilities of FH-RSVP. We first show that, by NS simulator, our FH-RSVP can achieve better QoS guarantee than MRSVP in terms of packets loss, handover latency and throughput. Generally, we show that FH-RSVP outperforms MRSVP in terms of reservation blocking, forced termination and session completion

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES SIGLES ET ABRÉVIATIONS

Sigle ou abréviation	Signification
MIPv6	Mobile IPv6
HMIPv6	Hierarchical Mobile IPv6
FMIPv6	Fast Mobile IPv6 (La relève rapide)
MN	Mobile Node (Nœud mobile)
CN	Corresponding Node (Nœud correspondant)
HA	Home Agent
MAP	Mobility Anchor Point
AR	Access Router (Routeur d'accès)
HAddr	Home Address (Adresse IP permanente du MN dans son réseau d'origine)
CoA	Care-of-Address (Adresse dynamique du MN dans le sous-réseau visité)
BU	Binding Update (Message d'enregistrement au HA)
QdS	Qualité de Service
RSVP	Resource ReSerVation Protocol

FH-RSVP	Fast and Hierarchical Mobile IPv6 RSVP
MRSVP	Mobile RSVP
HMRSVP	Hierarchical Mobile RSVP

CHAPITRE I
INTRODUCTION

Mobile IP [21] dans sa dernière version Mobile IPv6 [1] apparaît comme l'un des protocoles les plus prometteurs de l'Internet mobile de prochaine génération. De plus, avec l'augmentation de la largeur de bande des communications sans fil, des services IP multimédia en temps réel tels que la vidéo conférence, les jeux interactifs ou la téléphonie sur IP devront être supportés dans un futur proche. L'Internet mobile actuel ne fournit pas encore la qualité de service adéquate pour permettre le déploiement effectif de telles applications sur ces puissants outils mobiles.

Ce mémoire traite d'un mécanisme permettant de garantir la qualité de service (QdS) d'un flot de trafic d'applications temps réel échangé entre un nœud mobile et son nœud correspondant, tout en tenant compte de la micro-mobilité du nœud mobile. Dans ce chapitre d'introduction, nous définirons d'abord quelques concepts de base et les éléments de la problématique, ensuite nous préciserons nos objectifs de recherche et résumerons les résultats attendus, enfin nous esquisserons les grandes lignes du mémoire.

1.1 Définitions et concepts de base

La Figure 1.1 montre l'architecture d'un réseau Mobile IPv6 ainsi que ses principales composantes. Le protocole Mobile IPv6 (MIPv6) offre un mécanisme transparent de gestion de la mobilité d'un nœud mobile (MN) dans un environnement mobile IP. Ce protocole permet à un nœud mobile (MN), après un changement de son point d'attache d'un sous-réseau IP à un autre, de continuer à communiquer avec d'autres nœuds, ses nœuds correspondants (CNs), sans changer son adresse IP. Sans cette particularité, le nœud MN ne serait pas en mesure de maintenir les sessions des protocoles de couche supérieure et de transport, qui dépendent d'une adresse IP statique.

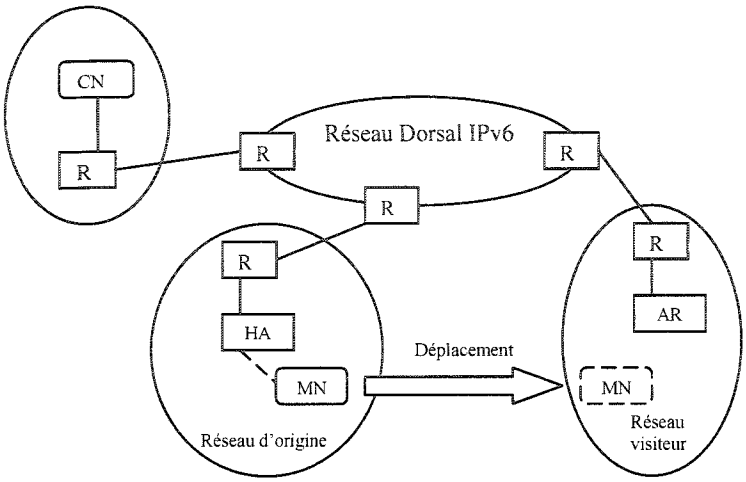


Figure 1.1 Architecture Mobile IPv6

Ce problème d'adressage est résolu en assignant deux adresses IP à un hôte mobile: une adresse IP permanente qui est appelée *Home Address (HAddr)*, et une adresse temporaire, dite *Care of Address* (*CoA*) qui est assignée à chaque fois que le nœud mobile visite un sous-réseau étranger. L'adresse *Home Address* est utilisée pour les sessions de la couche supérieure et de transport, tandis que la *CoA* est indispensable pour router correctement les paquets vers le point d'attache courant. De cette manière, l'impact de la mobilité de l'hôte est présent seulement dans la couche de routage et est maintenu transparent aux protocoles des couches supérieures dont la couche Transport.

Un agent, nommé *Home Agent* (HA), est un routeur dans le réseau d'origine du MN, prenant en charge la mobilité du MN. Chaque fois que le MN acquiert une nouvelle CoA, il doit s'enregistrer auprès du HA et de ses CNs, en transmettant des messages BU (Binding Update) de mise à jour. Les paquets de nouveaux appels émis par le CN sont interceptés par le HA et retransmis à l'intérieur d'un tunnel vers la CoA du MN en utilisant l'encapsulation IPv6, cela correspond au routage triangulaire, tandis que les paquets appartenant aux sessions actives sont transmis directement vers la CoA par un routage optimal. Les paquets provenant du MN sont transmis au CN à travers l'Internet.

La procédure de relève (*handover ou handoff*) est un processus qui permet à un MN, pendant qu'il est en communication, de changer son point d'attache d'un routeur d'accès (AR) à un autre. Une relève peut se produire de différentes façons : on distingue la relève de niveau 3 (couche réseau) et la relève de niveau 2 (couche connexion). La relève de niveau 2 est une opération engendrée par un MN qui change de point d'accès radio. Cette relève peut impliquer ou non une relève de niveau supérieur selon le type de connexion de liens des points d'accès radio (i.e., s'ils sont ou non sur la même connexion réseau).

Dans le cas de la relève de niveau 3, le MN a besoin d'obtenir une nouvelle adresse IP. Cela nécessite donc des messages d'enregistrement, ce qui peut occasionner une interruption de la communication. Le temps d'interruption peut augmenter avec le nombre d'usagers. Pour des applications en temps réel ou du trafic sensible au délai, il est important de recourir à des mécanismes plus fiables.

Ces délais sont directement reliés au temps aller-retour des messages d'enregistrement. Le temps entre le dernier moment où le MN peut recevoir et transmettre des paquets par l'intermédiaire de l'ancien *routeur d'accès* et le moment où la réception et la transmission de paquets peuvent débuter par l'intermédiaire du nouveau routeur d'accès se nomme le temps de latence d'une relève. Ainsi, c'est le temps durant lequel le MN ne peut ni recevoir ni transmettre du trafic IP. Ce temps permet d'évaluer les performances de la relève.

En vue d'améliorer les performances de mobile IP et en particulier le processus de *handoff*, de nouveaux protocoles complémentaires *Fast Mobile IPv6* (FMIPv6) [5] et *Hierarchical Mobile IPv6* (HMIPv6) [6] de gestion de mobilité ont été développés. Ces protocoles permettent de combler certaines faiblesses de MIPv6 comme la surcharge des messages de signalisation, la perte de paquet, et le délai de transmission d'un paquet.

1.2 Éléments de la problématique

L'une des insuffisances particulières de l'Internet actuel est le manque de qualité de service. La qualité de service est un concept ambigü donnant lieu à diverses

interprétations. En fait, deux facteurs importants n'avaient pas été considérés lors de la conception des unités mobiles quelques années auparavant : la mobilité et la garantie de qualité de service (QdS). En effet les deux modèles de QdS proposés par *l'Internet Engineering Task Force* (IETF) à savoir la réservation de ressources (*Integrated Service*) [2], [14] et la priorisation (*Differentiated Service*) [3], [9] ont été surtout développés au départ pour des environnements fixes (réseaux et hôtes fixes). Ainsi, ces protocoles ne sont pas complètement adaptés à des environnements mobiles, et particulièrement lorsque Mobile IP est utilisé comme le protocole de gestion de la mobilité. De nombreux travaux ont été réalisés [7], [10], [11], [12], [13], [18], [22], [23] et continuent d'être effectués à travers le monde afin de pouvoir concilier ensemble la gestion de la mobilité et la qualité de service.

Un usager mobile qui se retrouve à l'intérieur d'une zone fait des requêtes de service au réseau; par conséquent, le réseau a besoin d'offrir une certaine garantie sur la qualité de service de ces requêtes. Ainsi, pour des applications en temps réel et commerciales telles que la téléphonie IP et la vidéo en ligne dont les principaux paramètres de QdS sont le délai de transmission du paquet, le taux de perte de paquets, la gigue et le débit, la qualité de service est primordiale et doit être garantie. Afin de supporter des services en temps réel, le réseau doit être conçu pour offrir des garanties suffisantes sur ces paramètres de QdS.

La satisfaction de la qualité de service durant les relèves du MN demeure toujours un défi majeur. En effet, la mobilité d'un hôte a un impact significatif sur ces paramètres de QdS. Lorsqu'un nœud mobile se déplace d'un routeur d'accès à un autre avec un flot de données actif, le chemin emprunté par le flot de données peut être différent.

À la Figure 1.2, le nœud mobile se trouve au départ dans son réseau d'origine près du HA. Avant d'établir une session de communication entre le MN et le CN, il est crucial de réserver suffisamment de ressources de bout en bout sur le chemin correspondant à l'ancien chemin. Après avoir réservé ces ressources, le CN et le MN peuvent communiquer et la QdS est garantie sur ce chemin. Si, en cours de communication, le

MN veut effectuer une relève pour se retrouver dans un réseau visiteur, il s'agit alors de pouvoir mettre à jour et réserver de nouvelles ressources sur le nouveau chemin pour garantir la QdS. La mobilité d'un nœud mobile a donc un impact sur les paramètres de QdS des applications échangées (voix, vidéo..). En effet, le délai du paquet peut changer à cause des changements de la longueur du chemin et des différents niveaux de congestion au niveau des routeurs le long du nouveau chemin. Si la nouvelle position dans laquelle l'hôte mobile se retrouve est surchargée, la bande passante disponible dans la nouvelle localisation peut être insuffisante pour offrir le débit qu'il était en train de recevoir à la position précédente. De plus, l'hôte mobile peut subir des interruptions temporaires de service au cours de la relève pendant que la connexion est retirée le long de l'ancien chemin et est établie le long du nouveau chemin

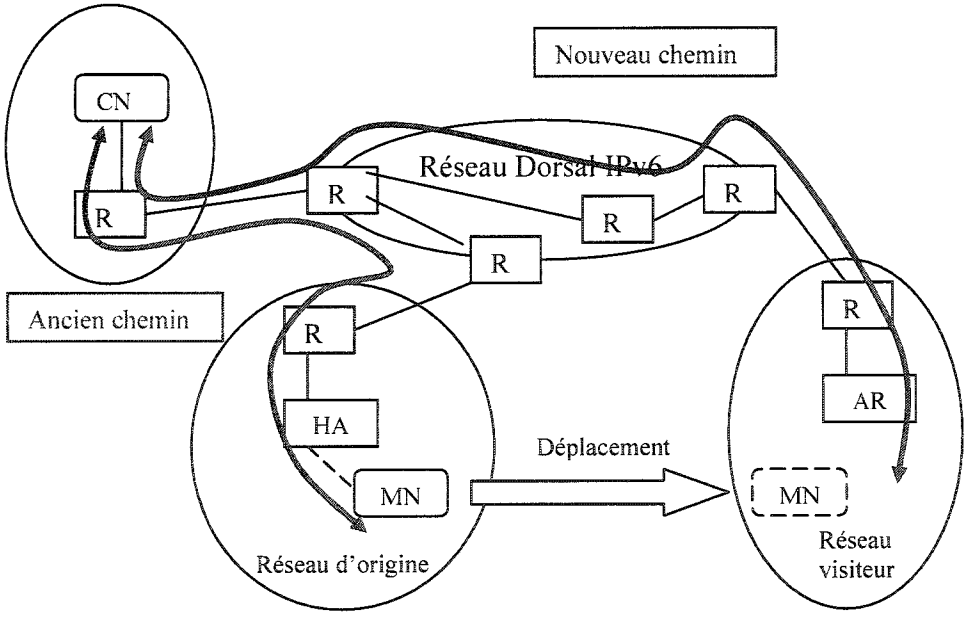


Figure 1.2 Impact de la mobilité du nœud MN sur la QdS

Avec l'introduction des nœuds mobiles, les routes changent du moment que les MNs s'attachent à d'autres sous-réseaux et obtiennent de nouvelles adresses IP. Ainsi, des ressources réservées aux nœuds intermédiaires de l'ancienne route doivent être

relâchées sur certains nœuds, et maintenues aux nœuds communs entre l'ancienne route et la route nouvellement sélectionnée. La situation est d'autant plus complexe lorsque les deux nœuds qui communiquent sont mobiles.

Ainsi, le réseau doit s'adapter à tous ces changements lorsque les usagers mobiles se déplacent avec leurs flots d'informations actifs. Pour des flots de données échangés entre le MN et le CN, deux types de migration de flots sont alors possibles. Le premier cas correspond à un flot de paquets émis d'un CN vers le MN. En effet, dans le protocole *Mobile IPv6 de base*, un nœud CN ne connaît pas la CoA du MN lorsqu'il envoie un flot de paquets de données vers le MN. Les paquets sont transmis vers le HA et le routage triangulaire est réalisé pour envoyer le flot de paquets de données. C'est seulement après réception d'un message BU provenant du MN que le CN peut directement transmettre des paquets de données vers le MN le long du chemin obtenu par le routage optimal. Dans ce scénario, le chemin de routage change de manière drastique d'un routage triangulaire à un routage optimal au cours de la session de flot de paquets de données. Il en résulte une sévère dégradation de la QdS. De plus, la dégradation devient plus importante lorsque le processus de relève se produit très fréquemment. Dans le protocole MIPv6, un changement du CoA du MN doit être directement transmis vers le CN en utilisant les messages BU. Cela implique que le CN ne peut optimiser les chemins de routage très rapidement, parce que le délai de signalisation devient très grand lorsque le MN est éloigné du CN. La réinitialisation du chemin de QdS est d'autant plus difficile car tous les nœuds le long du chemin doivent être encore initialisés en utilisant la signalisation de QdS (ex : mécanisme de signalisation RSVP).

Le second scénario de migration de flots de paquets correspond à un flot établi du MN vers le CN. Par exemple, dans un réseau d'accès sans fil composé de différentes technologies d'accès telle que UMTS et LAN sans fil, les zones de couverture peuvent se chevaucher. Avec de tels réseaux d'accès hétérogènes, le besoin et l'opportunité de choisir parmi un certain nombre de points d'accès possibles peuvent se présenter, en

particulier lorsqu'un nœud mobile MN a établi des flots de paquets avec des requis de QdS. Il serait préférable d'effectuer une procédure de relève seulement lorsque la QdS de ces flots peut être aussi bien garantie après le handoff.

Après analyse de ces problèmes de QdS, nous pouvons donc conclure que, dans les environnements *Mobile IP*, les services temps réel nécessitent un bon mécanisme de gestion de la mobilité et de la QdS.

La réservation de ressources est indispensable pour garantir de la QdS aux applications d'hôtes mobiles. Ainsi, plusieurs solutions adressant la gestion des ressources afin de garantir les requis de QdS pour des hôtes mobiles ont été proposées, à savoir la réservation en avance, l'extension du protocole *Mobile IPV6* avec l'option du *QOS OBJECT* [23] et la combinaison de MIPv6 et de RSVP. Dans le but de réaliser de la réservation par anticipation, plusieurs propositions ont été faites dont le protocole MRSVP [13]. L'un des défis majeurs de tels mécanismes est de pouvoir prédire les déplacements du nœud mobile de façon à ce que la réservation par anticipation soit faite à l'intérieur de zones potentielles. Cela résulte en des protocoles trop complexes et coûteux.

Bien que le protocole RSVP soit un protocole de signalisation bien mature, il ne s'adapte pas parfaitement aux environnements mobiles car il a été conçu au départ pour des environnements fixes. Plusieurs travaux ont été faits en vue de comprendre l'interaction entre IP mobile et RSVP. Shen et al. [22] ont amélioré RSVP afin de supporter de la signalisation pour la QdS dans *Mobile IP* en introduisant un identificateur de flot durant la relève pour l'interaction entre RSVP et IP mobile, en utilisant les avantages de la procédure de RSVP aller-retour (Path/Resv) pour initialiser la réservation de ressources sur le nouveau chemin durant les relèves. Ces approches combinant RSVP et *Mobile IP* ont des problèmes d'évolutivité et de surcharge de la signalisation.

L'option du *QOS OBJECT* développée par Chaskar et al. [23] est une nouvelle option d'entête de paquet IPv6 (*HOP BY HOP*), composée d'un ou de plusieurs objets de QdS nommé *QOS OBJECT.* Cette option peut être attachée aux messages

d'enregistrement BU et messages d'accusé de réception de BU Ack afin de transporter l'information de QdS pour les flots IP entre un MN et ses CNs. L'option de *QOS OBJECT* déclenche les actions nécessaires pour initialiser le traitement de la transmission de la QdS le long du nouveau chemin.

Ce mécanisme n'a pas été bien accueilli par la communauté scientifique bien qu'il permette de réduire le temps de latence pour que les paquets reçoivent un traitement de QdS adéquat. En effet, il utilise un mécanisme de signalisation de la QdS *in band*, ce qui pose d'énormes problèmes de sécurité. D'autre part, cette approche ne permet pas de sélectionner un autre routeur d'accès dans le cas de ressources insuffisantes le long de la route entre le MN et le CN.

Pour répondre aux besoins croissants des usagers mobiles qui exigeront d'avoir le même niveau de QdS que dans un environnement fixe, il est nécessaire d'explorer davantage ces méthodes ainsi que d'autres afin de dériver un nouveau mécanisme qui s'adapte mieux aux exigences des usagers.

1.3 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir une solution de QdS permettant de garantir la réservation de ressources pour des applications en temps réel échangés entre le nœud mobile (MN) situé dans un medium radio WLAN et le nœud correspondant (CN) en tenant compte du processus de *handoff* intra-site du nœud MN. De manière plus spécifique, ce mémoire vise à :

- analyser les problèmes liés à la QdS associée à un flot de paquets échangé entre le MN et le CN en prenant en compte le facteur de mobilité du MN dans le contexte de la micro-mobilité ;
- proposer un mécanisme qui permet de réserver des ressources pendant la relève pour un flot de données actif et établi avec une certaine politique de QdS que l'on désire au moins satisfaire après une relève du MN ;

- évaluer l'efficacité de la méthode proposée, en regard des méthodes existantes dans la littérature.

1.4 Plan du mémoire

Ce mémoire comprend 5 chapitres. Le chapitre suivant rappelle les différents protocoles de gestion de mobilité utilisés dans les environnements mobile IPv6, puis expose la problématique de l'impact de la mobilité d'un nœud mobile sur la QdS d'un flot actif de paquets temps réel et présente les différentes approches utilisées pour résoudre ce problème dans la littérature. Le chapitre 3 décrit l'approche que nous proposons pour résoudre ce problème. Le chapitre 4 présente les détails d'implémentation de notre algorithme ainsi que l'analyse détaillée des résultats assortie de comparaisons avec d'autres méthodes explorées pour la solution de QdS. Enfin, le chapitre 5 résume les principaux résultats obtenus, les limitations de la méthode proposée et les extensions possibles aux travaux déjà entrepris.

CHAPITRE II
QUALITÉ DE SERVICE DANS LES RÉSEAUX MOBILE IPv6

L'accès sans fil avec le protocole IP sera de plus en plus fréquent dans les réseaux de prochaines générations. Les usagers mobiles exigeront alors d'avoir la même qualité de service que celle offerte aux usagers des stations fixes. D'autre part, les protocoles de gestion de la QdS utilisés dans un réseau mobile IP ont démontré leurs limites dans un tel environnement mobile. Dans ce chapitre, nous faisons une synthèse de certains travaux de recherche sur la qualité de service dans les réseaux *Mobile IP* [21]. Nous débuterons par une description du protocole *Mobile IPv6*, puis des protocoles complémentaires de gestion de mobilité à Mobile IPv6 tels que FMIPv6 (*Fast Mobile IPv6*) et HMIPv6 (*Hierarchical Mobile IPv6)* qui permettent une meilleure gestion de la mobilité d'un nœud mobile, nous présenterons ensuite le paradigme qualité de service (*QdS*) et mobilité (basé sur le protocole MIPv6) en rappelant d'abord les principaux protocoles de QdS, puis en présentant les différentes méthodes utilisées dans la littérature pour garantir la réservation de ressources suffisantes dans un tel environnement mobile. Enfin, nous terminerons en soulignant un certain nombre de défis majeurs à relever en matière de QdS dans un réseau *Mobile IPv6*.

2.1 Caractérisation du protocole Mobile IPv6

Pour comprendre le fonctionnement du protocole *Mobile IPv6*, il est d'abord important de connaître le rôle de chaque entité qui le compose : MN, CN, HA et AR.

MN (Mobile Node) : le MN représente l'usager mobile dans le réseau. En effet, il peut être un routeur ou un nœud mobile qui peut changer son point d'attache d'un réseau ou d'un sous-réseau à un autre sans interrompre les connexions courantes et sans changer d'adresse IP.

CN (Correspondent Node) : le CN est un nœud du réseau qui communique avec l'usager mobile. Il peut être mobile ou stationnaire.

HA (Home Agent) : le HA est un système hôte ou un routeur situé dans le réseau d'origine du nœud mobile. Il maintient une trace sur la localisation des usagers mobiles (MNs), en établissant une correspondance entre les adresses fixes et les adresses dynamiques. L'agent HA intercepte et achemine directement les paquets destinés aux usagers en déplacement dans le réseau.

AR (Access Router) : c'est le routeur par défaut du MN. Le AR agrège le trafic externe des nœuds mobiles.

On distingue deux types de lien : lien visité et lien d'origine. Par lien visité, on entend tout lien qui ne se trouve pas dans le réseau d'origine du nœud mobile. Le lien d'origine est celui sur lequel le préfixe sous-réseau du réseau d'origine du MN est défini. Les mécanismes standard de routage IP transmettront les paquets destinés à l'adresse d'origine du MN sur ce lien.

La Figure 2.1 présente un scénario classique de Mobile IPv6 [1]. Ce scénario montre trois liens (A, B et C) et trois systèmes (MN, HA et CN). Le routeur placé sur le lien A offre les services d'un HA. Ce lien A est également le lien d'origine du MN.

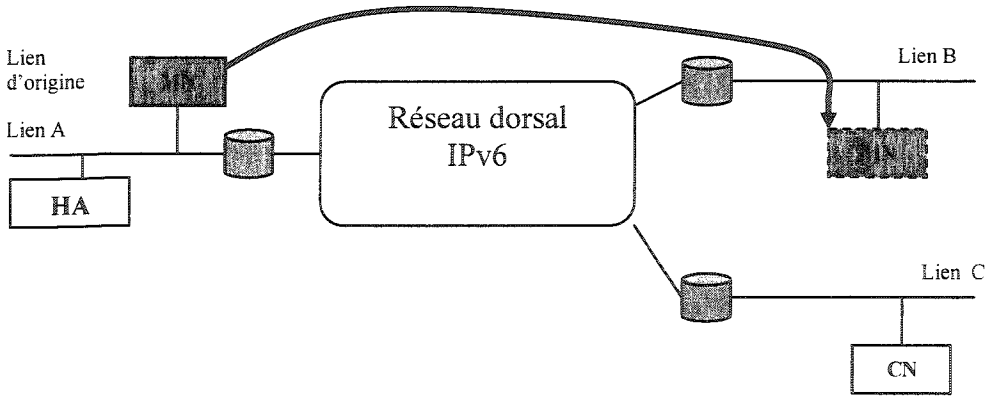


Figure 2.1 Scénario de Mobile IPv6

Dans ce scénario, le nœud mobile vient de se déplacer du lien A vers le lien B. De plus le nœud présent sur le lien C joue le rôle du CN. Le nœud correspondant CN peut être mobile ou stationnaire.

À chaque nœud mobile est assignée une adresse IP permanente (*Home Address* ou *HAddr*) qui est une adresse globale et connue par les nœuds correspondants. Lorsque le nœud mobile se déplace, la *Home Address* reste inchangée indépendamment de l'endroit où le MN est rattaché à l'Internet. L'agent HA est responsable de la gestion des paquets de données destinés au MN lorsque le nœud mobile est en dehors de son sous-réseau d'origine. Les paquets de données sont encapsulés et transmis au sous-réseau étranger courant auquel le MN est attaché. Cette procédure correspond au *tunneling* [28]. Par contre, le MN peut communiquer directement avec son nœud correspondant (CN).

Deux adresses IP sont assignées à chaque nœud mobile à son interface lorsqu'il est hors de son sous-réseau mère. La première adresse ou *Home Address* est une adresse assignée de façon permanente dont l'assignation est identique à une adresse IP. Elle est utilisée pour recevoir et envoyer les paquets aux autres usagers sur Internet ou sur un intranet. Les logiciels utiliseront toujours cette adresse pour démarrer ou recevoir une nouvelle connexion. La seconde adresse ou CoA (Care-of-Address) est une adresse dynamique qui possède le même préfixe que le sous-réseau visité auquel le MN est attaché. Cette adresse est associée à un MN lorsqu'il visite un réseau étranger et est assignée par le MN. La CoA est une adresse valide d'un lien ou réseau étranger que le MN utilise temporairement comme le point de sortie du tunnel à travers lequel le HA transmet les paquets au MN. Les préfixes sous-réseau sont au nombre de deux: le préfixe du sous-réseau d'origine qui est le préfixe sous-réseau IP correspondant à l'adresse d'origine du MN et le préfixe du sous-réseau visité qui désigne tout préfixe sous-réseau IP différent du préfixe du sous-réseau d'origine du MN.

- **Enregistrement au HA**

L'association de la *Home Address* avec la *Care-of-Address* du MN avec son temps d'association représente le *Binding*. Le MN est responsable de mettre à jour le HA sur son adresse CoA courante qui est globalement routable. Dès que le MN détecte qu'il s'est déplacé d'un lien vers un autre et qu'il découvre un nouveau routeur d'accès par défaut, il réalise une auto-configuration d'adresse de type *statefull* ou *stateless*.

Dans l'auto-configuration d'adresse *statefull*, c'est le MN qui crée son adresse CoA tandis que dans le cas *stateless* c'est plutôt le réseau. Tous les paquets destinés à l'adresse CoA parviendront au MN sur le lien courant. Le MN enregistre son adresse CoA à son HA situé sur le lien d'origine. En effet, à la Figure 2.2, le nœud mobile envoie un paquet à son HA contenant un message BU. Le HA enregistre cette association et envoie un paquet avec un message BU ACK au MN.

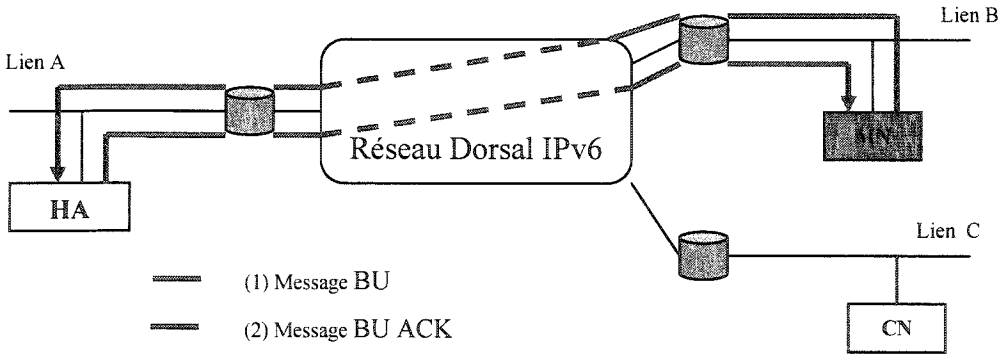


Figure 2.2 Enregistrement du nœud mobile MN auprès de son HA

Un MN peut utiliser une combinaison de mécanismes pour détecter son déplacement d'un lien à un autre. Une possibilité est d'attendre les messages *Router Advertisements* (*RA*) envoyés périodiquement. Ainsi, si le MN ne reçoit pas de *RAs* pour un certain temps, il assumera que son routeur par défaut n'est plus joignable et décidera d'utiliser un autre routeur pour lequel il peut recevoir désormais des *RAs*.

- **Le routage triangulaire**

Dès que le MN finit d'enregistrer son adresse *CoA*, le HA peut maintenant intercepter tout paquet destiné à la *Home Address* du MN. En utilisant un proxy de type *Neighbor Discovery* [1], le HA diffuse un message *Neighbor Advertisement* sur le lien d'origine. Ce message contient l'information sur l'adresse MAC de niveau 2 du HA pour l'adresse d'origine du MN. Le HA répond également à des requêtes de type *Neighbor Solicitations* adressées au MN. Chaque paquet intercepté est transmis par la création d'un tunnel vers la *CoA* enregistrée du MN, en utilisant l'encapsulation IPv6 [28]. Lorsque le nœud mobile veut transmettre des paquets à un nœud correspondant, il envoie directement les paquets à la destination du CN. Le MN initialise l'adresse source de ce paquet au CoA et inclut l'option de destination *Home Address*. Cela résulte en un routage triangulaire [1]. Le Figure 2.3 illustre le *routage triangulaire*.

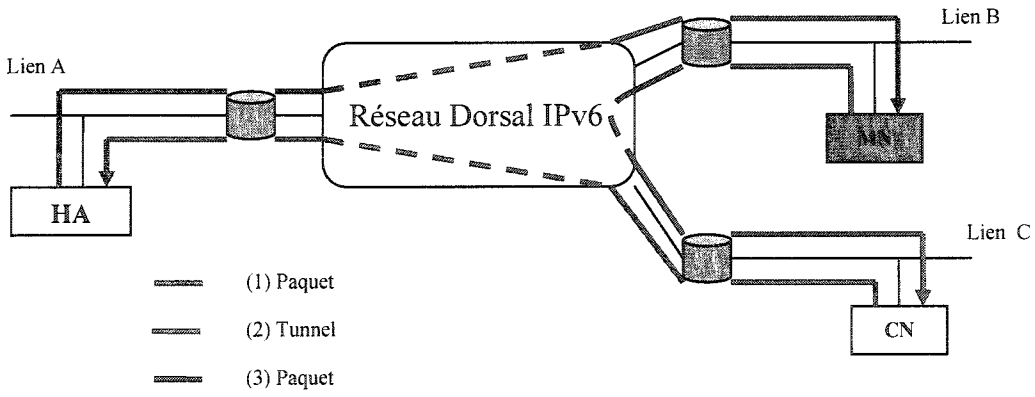


Figure 2.3 Routage triangulaire

Ainsi, lorsqu'un nœud MN en dehors de son réseau d'origine communique avec un nœud CN, les paquets transmis par le CN vers le MN sont routés du CN au HA, du HA au MN, tandis que le MN envoie directement les paquets au CN en utilisant le routage IP classique

- **Optimisation du routage**

Des méthodes d'optimisation du routage ont été proposées afin d'éviter le routage triangulaire [1]. L'optimisation du routage permet aux nœuds CN d'obtenir les adresses CoA des MNs. Pour ce faire, un MN doit envoyer des messages BUs à son nœud correspondant CN. Cela permet aux nœuds CN IPv6 d'avoir en mémoire (*Binding Cache*) l'adresse CoA courante et de transmettre directement les paquets au MN (Figure 2.4).

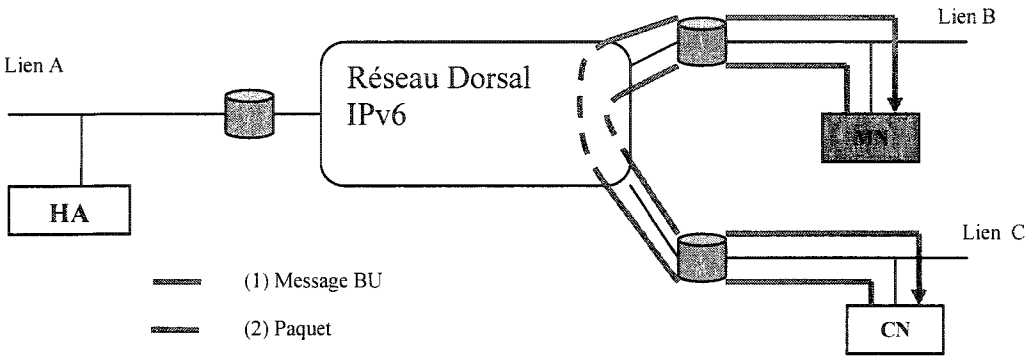


Figure 2.4 Optimisation du routage

Un nœud CN IPv6, qui veut envoyer un paquet, vérifie en premier dans son *Binding Cache* s'il existe une correspondance pour l'adresse de destination. Le *Binding Cache* est une liste de correspondance possédée par chaque nœud IPv6 qui est utilisée pour établir les correspondances avec les autres nœuds. Si la correspondance existe, le CN transmet le paquet au MN en utilisant une entête réseau (contrairement à l'encapsulation IPv6). La route spécifiée par cette entête réseau possède deux hops (sauts). Le premier hop est la CoA et le second est la *Home Address* du MN. En effet, le paquet est directement transmis au CoA du MN. Le nœud mobile reçoit ce paquet et le transmet au hop suivant, spécifié par l'entête réseau. Le hop suivant et final correspond à l'adresse d'origine du MN, ainsi le paquet reviendra au MN. Par la suite, le paquet sera traité comme si le MN était sur son réseau d'origine (Figure 2.5).

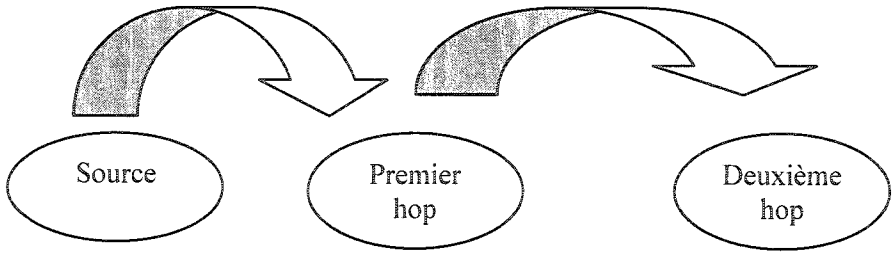


Figure 2.5 Entête réseau d'un paquet transmis directement au MN

S'il n'y a pas de correspondance trouvée dans le *Binding Cache*, le paquet sera transmis normalement. Ce paquet est ainsi routé vers le réseau spécifié et reçu par le nœud de destination. Dans le cas où la destination est un nœud mobile en dehors de son réseau d'origine, le paquet sera intercepté par le HA sur le lien d'origine qui crée le tunnel vers le MN.

2.2 Autres protocoles complémentaires à Mobile IPv6

En vue d'améliorer les performances de IP mobile et en particulier le processus de relève, certains protocoles de mobilité ont été développés. Ces protocoles permettent de combler certaines faiblesses de *MIPv6* comme la surcharge des messages de signalisation, la perte de paquet, et le délai de transmission d'un paquet.

2.2.1 Protocole Fast Mobile IPv6

Le mécanisme de *relève rapide (ou fast handover)* [5] est une amélioration du protocole MIPv6 qui permet au MN d'être connecté plus rapidement à un nouveau point d'attache lorsque le MN est en déplacement. Le *fast handover* est une solution qui permet de minimiser le temps nécessaire pour qu'un MN transmette ou reçoive des paquets IPv6 (i.e., le temps de latence des relèves). Le principe du *fast handover* est d'établir une nouvelle adresse temporaire avant que le MN ne rompe sa connexion avec son ancien routeur d'accès (*oldAR*). Ainsi, lorsque le mobile est relié au nouveau routeur d'accès (*newAR*), il peut continuer ses communications avec sa nouvelle adresse connue

d'avance. Si cet enregistrement anticipé échoue, le MN peut toujours réaliser une relève classique. Le *fast handover* définit donc une méthode de transmission de paquets entre le *oldAR* et le *newAR*. L'établissement d'une nouvelle adresse temporaire avant même que le nœud mobile se déplace implique une anticipation du mouvement du mobile. Cette anticipation peut se faire à l'aide des messages échangés au niveau physique ou plus simplement par l'information appropriée provenant du niveau 2 (mesure de la sensibilité du signal, etc....). L'objectif est de pouvoir réaliser la *relève* au niveau 3 avant que celle au niveau 2 soit terminée.

a) Terminologie Mobile IPv6

oldAR : c'est l'ancien routeur ou le AR d'accès impliqué dans la gestion d'un trafic MN avant la relève de niveau 2. Le *oldAR* est le routeur auquel le MN est actuellement attaché.

newAR : c'est le nouveau routeur d'accès ou le AR impliqué dans la gestion d'un trafic MN après la relève de niveau 2. Le *newAR* est le routeur vers lequel le MN s'en va.

oldCoA : c'est l'ancienne CoA à savoir la *CoA* avant le premier mouvement du MN.

newCoA : c'est la nouvelle CoA à savoir la *CoA* dans le nouveau sous réseau.

b) Description de FMIPv6

Plusieurs cas sont possibles lors de la *relève rapide* mais les sections qui vont suivre se basent essentiellement sur l'unique cas suivant où le *newAR* est connu du *oldAR*, le *newAR* accepte d'attacher le MN au nouveau sous-réseau. Ce cas s'applique en particulier à deux scénarios dans le réseau :

- *La relève initiée par le réseau (Network initiated Handover)* : le réseau détermine la relève (le *oldAR* choisit le nouveau point d'attache vers lequel le MN se déplacera). Le *oldAR* initie la signalisation vers le MN et le *newAR* afin de débuter la relève de niveau 3.

- *La relève initiée par le mobile (Mobile initiated Handover)* : le MN détermine la relève (le mobile doit détecter et débuter la relève). MN décide de forcer son déplacement vers un nouveau point d'attache. Le MN initie la signalisation vers le *oldAR* afin de commencer la relève.

b.1) La relève initiée par le réseau (Network initiated Handover)

Dans la relève initiée par le réseau à la Figure 2.6, le *oldAR* reçoit une indication sur le fait que le MN est sur le point de se déplacer et une information sur le *newAR* vers lequel le MN se déplacera. La configuration de la nouvelle adresse *newCoA* peut se faire de deux façons : une configuration de type *stateless* ou une de type *statefull*.

- **Cas d'une configuration de type *stateless* du CoA**

Dans cette configuration, lorsque le *oldAR* détecte à la Figure 2.7 que le MN doit se déplacer vers un nouvel AR, le oldAR crée une nouvelle CoA à partir de l'adresse MAC du nœud mobile (*Mobile ID interface*) et le préfixe du *newAR*. Il transmet ensuite la CoA au MN avec l'adresse IP du newAR et l'adresse de la couche liaison en utilisant des messages *Proxy Router Advertisement (PrRtAdv)*.

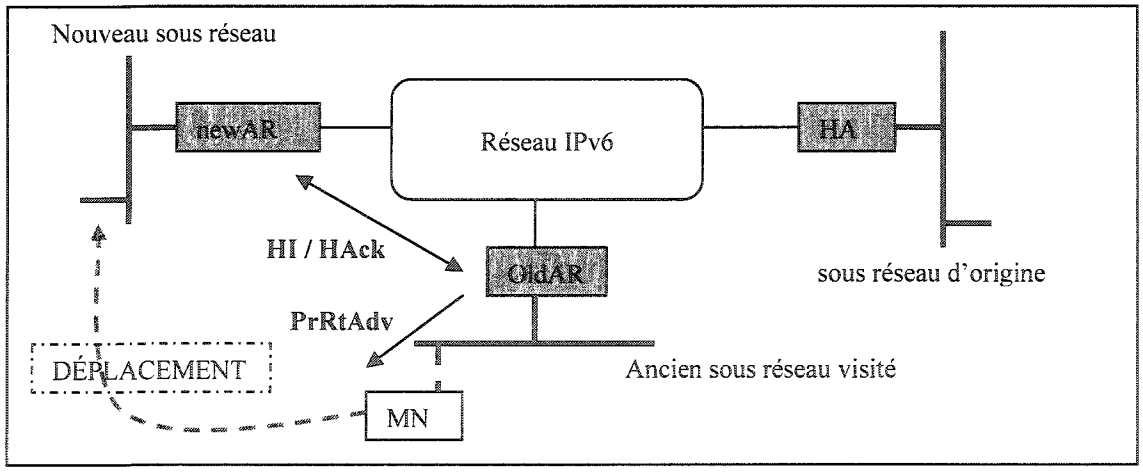


Figure 2.6 Relève initiée par le réseau (Network initiated Handover)

Au même moment, le *oldAR* envoie un message *Handover Initiated (HI)* au *newAR* en indiquant la *oldCoA* et la *newCoA* du MN.

Le *newAR* vérifie initialement si la *newCoA* est valide en s'assurant que l'adresse n'est pas utilisée par un autre mobile. Si la CoA est valide et acceptable par le *newAR,* alors le *newAR* ajoute la nouvelle adresse dans sa cache des visiteurs (*Neighboring Cash*) pour une courte période et renvoie un message *Handover Acknowledgement (HAck).* Si la nouvelle CoA n'était pas valide, le *newAR* doit indiquer dans le message HAck envoyé au oldAR que la *newCoA* n'est pas valide.

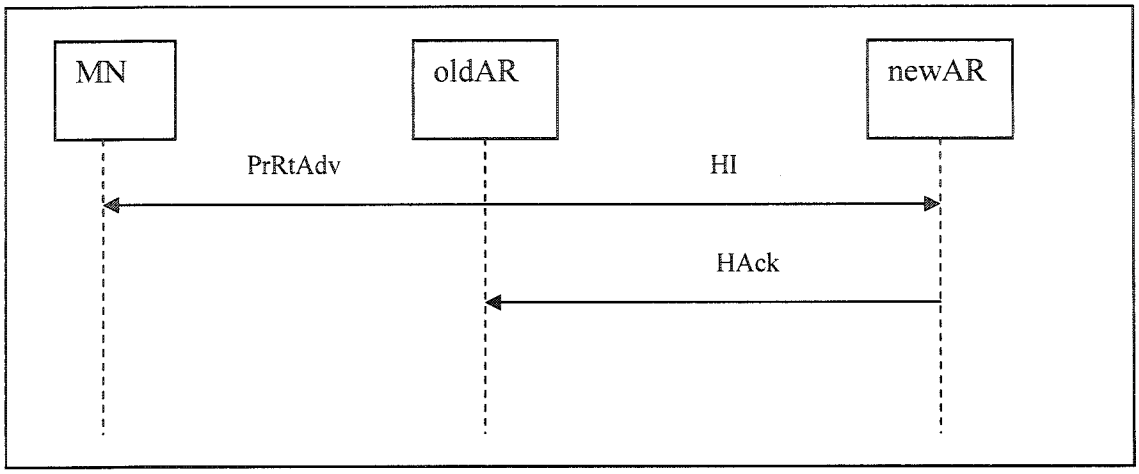


Figure 2.7 Échange de messages pour la configuration de type *stateless* du CoA

- **Cas d'une configuration de type *statefull* du CoA**

Dans cette configuration, le oldAR à la Figure 2.8 doit émettre un message HI avant le message *Proxy Router Advertisement (PrRtAdv).* Le message HI permet de demander une nouvelle adresse temporaire pour le MN sans la valider. Le message HAck contient une adresse valide qui peut être transmise au mobile dans le message *PrRtAdv.* Le *newAR* échange des messages avec le *oldAR* et propage les messages entre le *oldAR* et le MN. Lorsque le newAR reçoit HI sans une nouvelle CoA, il alloue alors une nouvelle CoA et le transmet au *oldAR* à l'intérieur du HAck. Dans le cas où le *newAR* reçoit HI avec une nouvelle CoA, il détermine si cette *newCoA* est valide et transmet une indication de validation dans le message HAck.

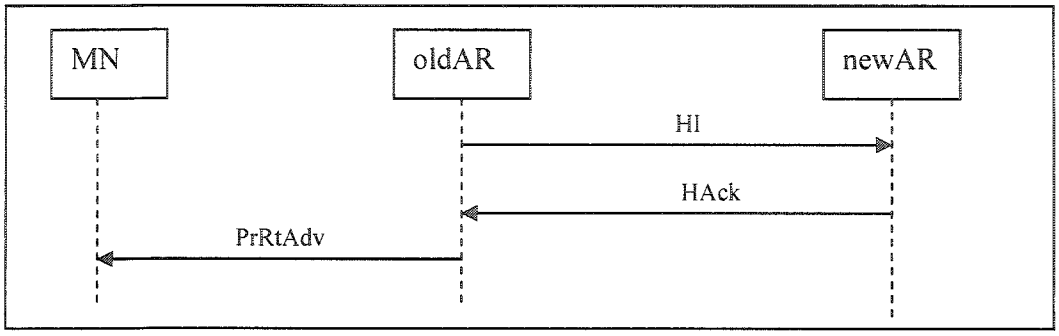


Figure 2.8 Échange de messages pour la configuration de type *statefull* du CoA

b.2) La relève initiée par le mobile (ou Mobile initiated Handover)

La différence majeure entre la relève initiée par le mobile illustrée à la Figure 2.9 et celle initiée par le réseau provient du fait que, dans la première, le MN reçoit l'information sur la relève de niveau 2. Pour initier le *fast handover*, le MN doit envoyer le message *Router Solicitation for Proxy* (*RtSolPr*) à son *oldAR* et ce dernier fera démarrer des messages *PrRtAdv*. Dans le message *RtSolPr*, le MN doit indiquer l'adresse de niveau 2 ou l'identificateur du point d'attache vers lequel il veut migrer.

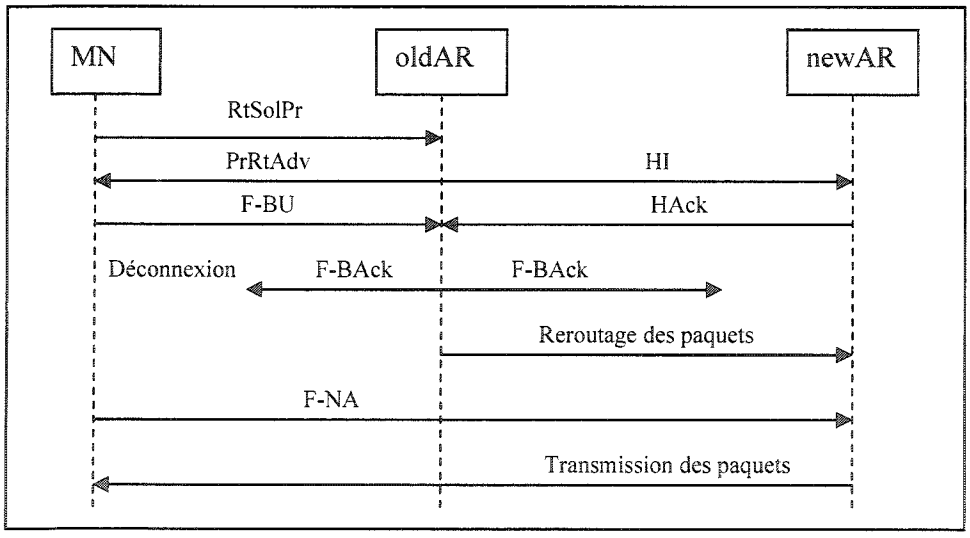


Figure 2.9 Relève initiée par le mobile

Le *oldAR* répondra avec un message *PrRtAdv* qui contient la même information que celle décrite précédemment dans le cas de la relève initiée par le réseau. Les

messages qui suivent, dupliquent la séquence de la relève initiée par le réseau, avec les deux possibilités (*stateless* ou *statefull*) décrits ci-haut. La *newCoA* est transmis au *newAR* pour validation en utilisant les messages HI et HAck.

c) La procédure d'enregistrement

Lors de la procédure d'enregistrement, la relève initiée par le mobile et celle initiée par le réseau se comportent de la même manière. Après les descriptions de l'initiation de la relève, le MN envoie un message *F-BU (Fast BU)* au *oldAR* en utilisant sa CoA avant qu'il entame la relève. Cette rapide mise à jour (*Fast BU*) doit être effectuée pendant que le MN est toujours connecté au *oldAR*. Le *oldAR* doit envoyer un message d'accusé de réception *Fast BAck* vers le MN en utilisant de façon locale la *newCoA* ou par l'intermédiaire de l'adresse d'encapsulation du *newAR* (voir Figure 2.10). Le *oldAR* peut maintenant débuter l'envoi de paquets pour le MN à son adresse CoA ou à son *newCoA* ou au *newAR* selon la valeur du message HAck.

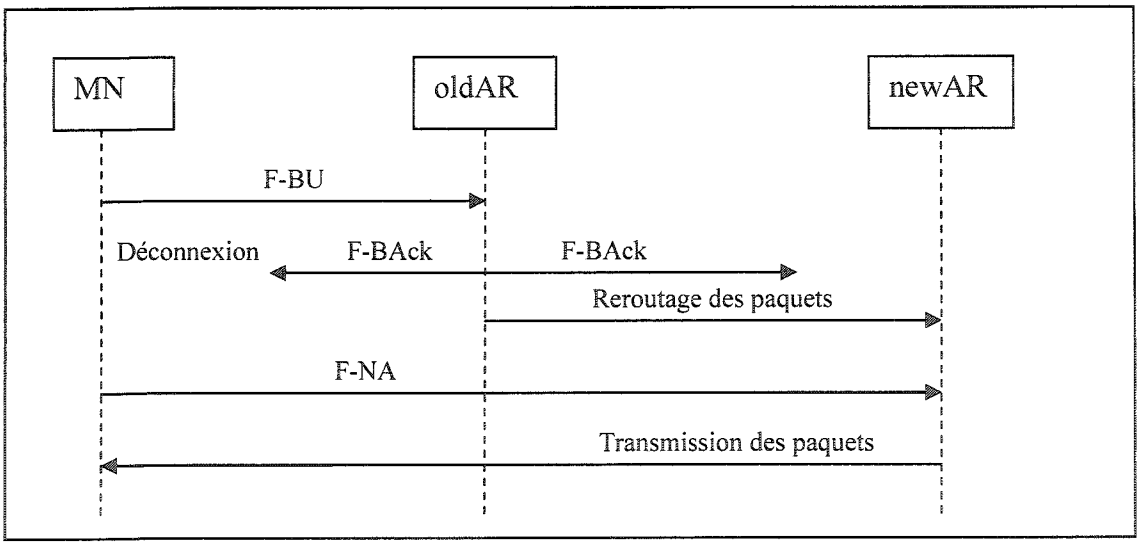


Figure 2.10 Messages d'enregistrement échangés

En effet, si le message HAck indique que la *newCoA* est valide, alors le *oldAR* enverra les paquets au MN avec sa *newCoA*. Dans le cas contraire, le *oldAR* utilisera le *newAR*. Si la couche connexion le permet, le *oldAR* peut retarder le routage jusqu'à la

déconnexion au *oldAR* du MN. Le *oldAR* se comporte comme un HA avec une adresse locale (*oldCoA*) et une adresse CoA (*newCoA* ou l'adresse du *newAR*).

Lorsque le MN arrive sur le newAR, il envoie un message F-NA (*ou Fast Neighbbor Advertisement)* pour initier le flot de paquets en attente. Finalement, après le déplacement du MN, le MN doit transmettre un BU à son HA et à ses CNs à travers le newAR afin d'enregistrer sa *newCoA*.

2.2.2 Protocole Hierarchical Mobile IPv6

Le protocole *Mobile IPv6* décrit précédemment permet à des nœuds de se déplacer à l'intérieur d'une topologie Internet tout en maintenant leur disponibilité et en fournissant des connexions entre les nœuds MN et CNs. Pour ce faire, le nœud mobile envoie chaque fois qu'il se déplace des BUs à son HA et à tous les nœuds correspondants avec qui il communique. L'authentification des BUs nécessite un temps approximativement égal à au moins 1.5 fois le temps d'un aller-retour entre le MN et chaque CN (pour une procédure complète de routabilité dans le meilleur des scénarios, i.e. sans perte de paquets). De plus, la mise à jour du HA demande au moins le temps d'un aller-retour. On a également un nombre de temps aller-retour nécessaire pour la mise à jour des différents nœuds CNs. Ces différents délais (en terme de temps aller-retour) occasionneront l'interruption des connexions actives à chaque fois que le MN changera de routeur d'accès. On parle de *relève* du MN pour indiquer le changement effectué par un MN lorsqu'il passe d'un routeur d'accès à un autre.

Afin d'améliorer les performances de IPv6 mobile et d'éliminer ce délai additionnel lors de la période critique de la relève du MN, le mécanisme de gestion de mobilité hiérarchique *HMIPv6* [6] a été développé par l'IETF comme complément à *Mobile IPV6*. Le protocole *HMIPv6* [17] a pour but principal d'améliorer la QdS [30] en limitant le nombre de messages de signalisation transmis à tous les CNs et au HA lorsque le MN se déplace dans le réseau, en introduisant une nouvelle entité physique, le *MAP* (*Mobility Anchor Point*). Un *MAP* est essentiellement un HA local, qui peut être placé à n'importe quel niveau d'un réseau hiérarchique de routeurs. Le *MAP* n'est pas

indispensable sur chacun des sous-réseaux. En effet, au lieu d'envoyer les BUs au HA qui est parfois très éloigné et aux CNs, le MN transmet les *Binding Updates* locaux uniquement vers le *MAP* local. Ainsi, lorsque le nœud mobile est en mouvement ou change de routeur d'accès, un seul message de BU doit être transmis par le MN avant que le trafic provenant du HA et de tous les CNs soit re-routé vers sa nouvelle localisation. Cela est indépendant du nombre de CNs communiquant avec le MN. Par exemple, dans le cas des réseaux sans fil, cette approche permet de réduire le nombre de messages transmis à travers l'interface air vers tous les CNs et le HA.

a) Terminologie HMIPv6

MAP (ou Mobility Anchor Point) : un *MAP* est un routeur situé dans un réseau visité par le MN. Le *MAP* est utilisé par le MN comme un HA local. Il peut exister un ou plusieurs *MAPs* à l'intérieur d'un réseau visité.

RCoA (Regional Care-of-Address) : une *RCoA* est une adresse sur le sous-réseau du *MAP* obtenue par le MN à partir du réseau visité. Elle est auto-configurée par le MN lorsqu'il reçoit l'option MAP.

MN_HMIPv6 (HMIPv6-aware Mobile Node) : le *MN_HMIPv6* est un nœud mobile qui peut recevoir et exécuter l'option MAP reçu à partir de son routeur par défaut. Le MN_HMIPv6 peut envoyer des messages BUs locaux.

LCoA (On-link CoA) : la *LCoA* est l'adresse CoA sur le lien configurée sur une interface du MN basée sur le préfixe donné par le routeur défaut du MN.

LBU (Local Binding Update) : le nœud mobile envoie un BU local (*LBU*) au MAP afin d'établir une association entre la *RCoA* et la *LCoA*.

b) Vue d'ensemble de *HMIPv6*

Le protocole *HMIPv6* introduit le *MAP* comme nouvelle entité et quelques modifications au mode d'opération du MN. Les modes d'opérations respectifs du HA et du CN dans IPv6 mobile restent inchangés dans HMIPv6. Un routeur de type

MN_HMIPv6 peut choisir d'utiliser le *MAP* lorsqu'il se retrouve dans un réseau visité offrant cette fonctionnalité ou décider dans certains cas d'utiliser les mécanismes standard de IPv6 mobile. Tout comme *Mobile IPv6*, *HMIPv6* est indépendant de la technologie d'accès sous-jacente. Un nœud mobile entrant dans un domaine du MAP reçoit des messages *Router Advertisements* contenant l'information sur un ou plusieurs *MAP* locaux (*RCoA).* Le MN peut alors associer son adresse de localisation courante (*LCoA*) à une adresse sur le sous-réseau du MAP (*RCoA*). Le *MAP* qui se comporte exactement comme un HA local recevra tous les paquets destinés au MN qu'il sert, puis encapsulera ces paquets pour enfin les transférer à l'adresse courante du MN. Si le nœud mobile change son adresse courante (*LCoA*) à l'intérieur d'un domaine *MAP* local, il a besoin seulement d'enregistrer la nouvelle adresse auprès du *MAP*. Ainsi, seule la *RCoA* doit se faire enregistrer auprès des CNs et du HA. La *RCoA* n'est pas modifiée aussi longtemps que le MN se déplace à l'intérieur d'un domaine du *MAP*. Les frontières d'un domaine du *MAP* sont définies par les routeurs ARs qui fournissent l'information sur le *MAP* aux nœuds mobiles qui sont reliés. La mobilité du MN devient donc transparente pour les nœuds CN avec lesquels le MN communique.

c) Modèles de hiérarchie de *HMIPv6*

Dans HMIPv6, on distingue deux modèles de hiérarchie : la hiérarchie à un niveau et celle multi-niveau.

- **Hiérarchie à un niveau (un domaine MAP)**

L'architecture de réseau de la Figure 2.11 illustre l'utilisation du *MAP* dans un réseau visité. Le *MAP* fournit une mobilité sans interruption dite *seamless* pour le MN lorsqu'il se déplace du routeur AR1 vers le routeur AR2, pendant sa communication avec le CN. Lorsque le MN arrive dans un réseau visité, il découvre l'adresse globale du *MAP* stockée dans les routeurs ARs et transmise au MN via des *RA*s (*Router Advertisements*). Cette procédure de découverte du *MAP* permet d'informer le MN sur la distance à laquelle il se trouve du *MAP*.

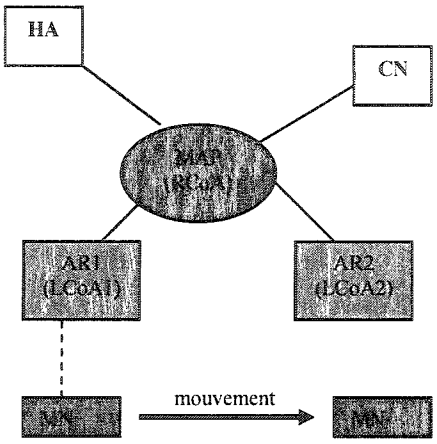


Figure 2.11 HMIPv6 utilisant un domaine (un MAP)

Les fonctionnalités du *MAP* peuvent être également implémentées dans AR1 et dans AR2 (voir Figure 2.11), ce qui correspond au cas de la hiérarchie multi-niveau. Le processus de découverte du *MAP* continue tant que le MN se déplace d'un sous-réseau à un autre. Comme le MN se déplace à l'intérieur d'un domaine *MAP*, les ARs sont configurés pour indiquer la même adresse *MAP* ou les mêmes adresses. Si le MN reçoit un changement d'adresse du *MAP*, il réalise la détection d'un mouvement et envoie les messages BUs à son HA et ses CNs.

Si le MN est un nœud *MN_HMIPv6*, le MN peut utiliser le protocole HMIPv6. Le MN découvre la localisation du *MAP* et s'enregistre auprès de ce dernier en envoyant un BU contenant son HAddr et son *LCoA*. La HAddr utilisée dans BU est la *RCoA*.

- **Hiérarchie multi-niveau (plus d'un domaine MAP)**

À la Figure 2.12 les *MAPs* structurés hiérarchiquement peuvent fournir une mobilité sans interruption dite *seamless* pour le MN lorsqu'il se déplace du *MAP2* vers le *MAP3*, pendant sa communication avec le CN. Cette hiérarchie dite multi-niveau permet de sélectionner plus d'un *MAP* et force les paquets à être transmis à partir du *MAP* supérieur, de haut vers le bas, en traversant une hiérarchie de *MAPs* (structure arborescente).

Lorsque le MN arrive dans un réseau visiteur, le MN enregistre la *RCoA1* avec le HA et les CNs. Il obtient la RCoA pour chaque niveau de la hiérarchie. Lorsque le MN se déplace vers le *MAP2*, il obtient *RCoA2* (à partir du MAP2) et *RCoA1* (à partir du *MAP1*). Si *MAP1* reçoit un paquet adressé à *RCoA1*, qui est la RCoA du MN situé au MAP1, il peut déterminer la RCoA suivant en analysant l'association entre le RCoA et le RCoA de niveau inférieur suivant. Par la suite, ce *MAP* transmet le paquet (par un tunnel) vers cette RCoA. Cela continue jusqu'à ce que le paquet atteigne le *MAP* de plus bas niveau. À la Figure 2.12, *MAP1* envoie le paquet vers la *RCoA2* (par un tunnel). *MAP2* décapsule le paquet, l'encapsule et l'envoie vers l'adresse *LCoA* du MN (par un tunnel).

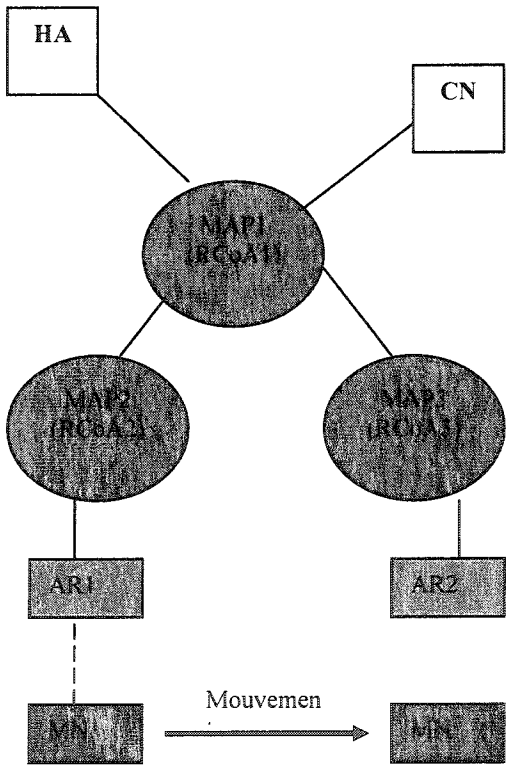


Figure 2.12 HMIPv6 utilisant une hiérarchie multi-niveau de MAPs

On distingue deux types de relève dans une hiérarchie multi-niveau :

- la relève inter-site : le MN se déplace d'un MAP vers un autre MAP et ces deux MAPs impliqués dans la relève se trouvent sur différents niveaux de hiérarchie (Ex : le MN se déplace du MAP1 vers le MAP2) ;
- la relève intra-site : le MN se déplace d'un MAP vers un autre MAP et ces deux MAPs impliqués dans la relève se trouvent sur un même niveau de hiérarchie (Ex : le MN se déplace du MAP2 vers le MAP3).

La Figure 2.13 présente un exemple de relève inter-site d'un MAP situé dans une région vers un autre MAP situé dans une autre région. Ainsi, à la Figure 2.13, le nœud mobile se déplace du MAP1 vers le MAP2. Nous décrivons également de façon détaillée les différents messages échangés lors de cette relève inter-site du nœud MN.

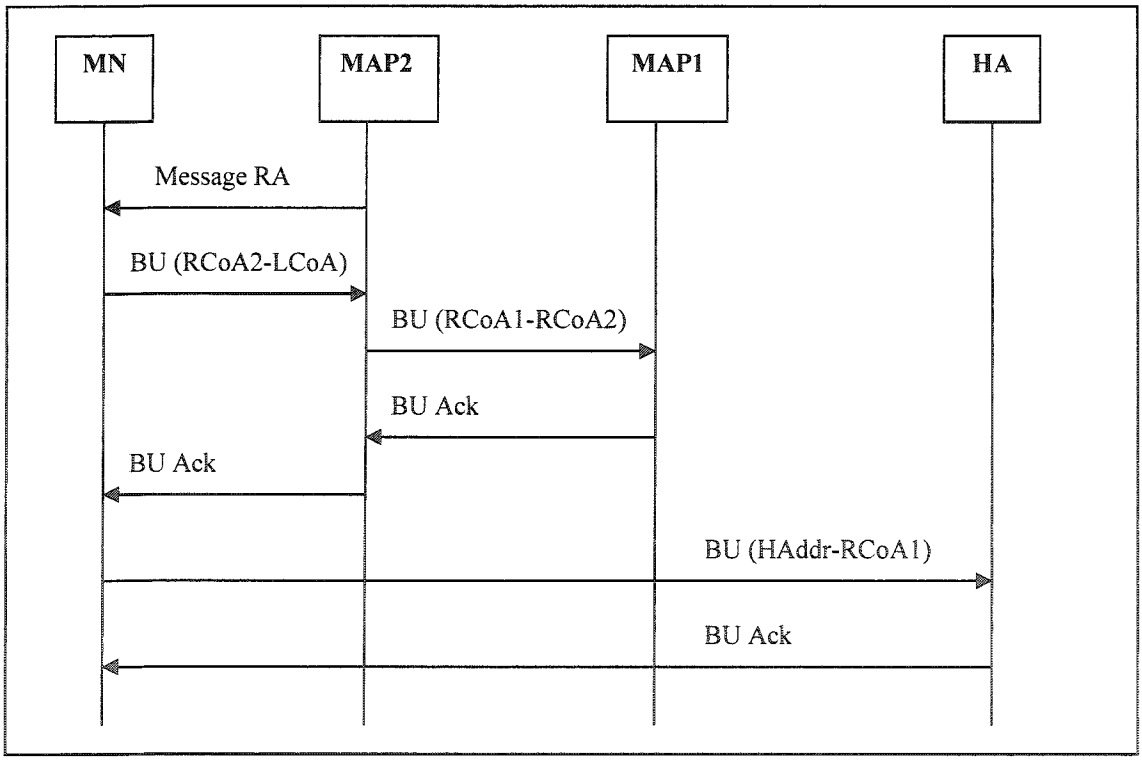


Figure 2.13 Procédure de handover inter-site

Description :

1. le MN reçoit un message *RA* (*Router Advertisement*) de *MAP2* indiquant une nouvelle hiérarchie ;
2. il envoie un BU pour associer son adresse *LCoA* à son adresse *RCoA (RCoA2)* de plus bas niveau, à son *MAP* de plus bas niveau (*MAP2*) ;
3. le *MAP2* envoie un BU pour associer la *RCoA2* au *RCoA (RCoA1)* du *MAP* de niveau supérieur (*MAP1*) ;
4. *MAP1* qui est le *MAP* du plus haut niveau envoie un BU Ack au *MAP2* ;
5. *MAP2* reçoit le BU Ack et l'envoie vers le MN ;
6. le MN reçoit le BU Ack et peut maintenant s'enregistrer auprès de son HA en envoyant un BU (association entre la *RCoA1* et son HAddr) ;
7. le HA reçoit le BU et renvoie un BU Ack.

D'autre part la Figure 2.14 présente un exemple de procédure de relève intra-site du MAP2 vers le MAP3 situés dans une même région.

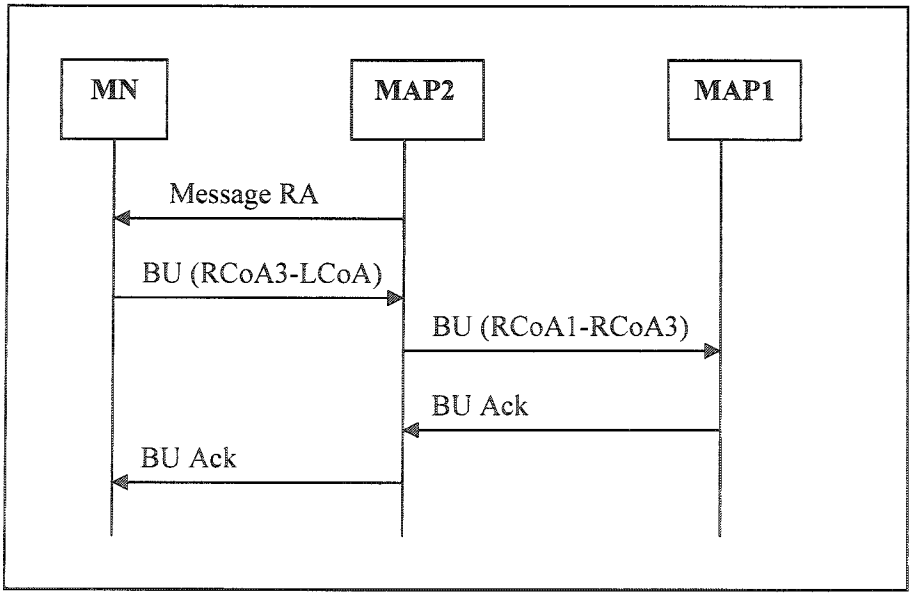


Figure 2.14 Procédure de handover intra-site

Description :

1. le MN reçoit un message *RA* (*Router Advertisement*) de *MAP2* et obtient une nouvelle adresse *LCoA* ;
2. il envoie un BU pour associer son adresse *LCoA* à son adresse *RCoA* de plus bas niveau (*RCoA3*), à son *MAP* de plus bas niveau (*MAP3*) ;
3. le *MAP3* envoie un BU pour associer la *RCoA3* au *RCoA* (*RCoA1*) du *MAP* de niveau supérieur (*MAP1*) ;
4. *MAP1* envoie un message BU Ack au *MAP3* ;
5. *MAP3* reçoit le BU Ack et l'envoie vers le MN ;
6. le MN reçoit le BU Ack.

NB : le MN envoie également des messages BUs aux CNs locaux qui ont besoin de connaître son changement de localisation. MN n'envoie pas de BU au HA et aux CNs qui sont à l'extérieur de la hiérarchie.

2.3 Mobile IPv6 et qualité de service

La qualité de service dans un réseau *Mobile IPv6* dépend de trois aspects essentiels : le premier est la mobilité du nœud mobile, le deuxième est la qualité de service associée aux paquets transmis entre le MN et le CN d'une part et entre le MN et le HA d'une autre part, le troisième dépend des paramètres propres de qualité de service des liaisons sans fil (pertes élevées de paquets, temps de latence élevée, gigue élevée). Dans un réseau *Mobile IP*, la QdS peut être établie à partir d'un ensemble de requis à garantir lors d'une session. Ces requis de QdS peuvent être spécifiés par des protocoles de QdS, ou peuvent se retrouver par exemple à l'intérieur de mécanismes tels que la gestion des ressources du réseau ou de la relève du MN. Ces protocoles de QdS ou mécanismes peuvent améliorer la performance du réseau de façon considérable.

2.3.1 Type de Qualité de service sur IP

Les principaux types de QdS se regroupent en deux grands paradigmes:

- *Réservation de ressources* (*Integrated Services* ou *IntServ*): les ressources du réseau sont réparties en fonction des garanties de QdS requises par chaque application et de la politique de gestion des ressources (largeur de bande). Un exemple de protocole serait RSVP qui fournit les mécanismes pour faire de la réservation de ressources.
- *Priorisation* (*Differentiated Services* ou *DiffServ*): le trafic réseau est classifié et les ressources du réseau sont réparties en fonction de la politique de gestion de largeur de bande. Pour garantir la qualité de service, les classifications offrent un traitement préférentiel aux applications identifiées comme plus d'exigeantes.

Ces types de QdS peuvent être appliqués aux flots de données (pour *Integrated Services*) d'une application individuelle ou aux agrégats de flots de données (pour *Differentiated Services*). Il est donc possible également de caractériser les types de QdS de la manière suivante :

- Par flot de données : un flot est défini comme un ensemble de données individuelles, unidirectionnelles entre deux applications (émetteur et récepteur), identifié de façon unique par un 5-tuplet (protocole de transport, adresse source, numéro du port de la source, adresse de destination, et numéro du port de la destination).
- Par agrégat de flots de données: un agrégat de flots de données est simplement constitué de deux ou plusieurs flots de données. En général, ces flots de données auront quelques particularités communes (ex : un ou plusieurs des paramètres du 5-tuplet, une étiquette ou un numéro de priorité ou peut être une information d'authentification).

Ces protocoles de signalisation de QdS pour IP ont été principalement conçus pour des environnements statiques (réseaux et systèmes hôtes fixes) et ne sont pas entièrement adaptés à des environnements mobiles, particulièrement lorsque IP mobile est utilisé comme le protocole de gestion de la mobilité. Ces deux architectures peuvent

être utilisées indépendamment ou l'une sur l'autre pour garantir la Qualité de Service. *DiffServ* possédant d'excellentes qualités d'évolutivité d'un point de vue réseau mais ne possédant pas de signalisation avec les applications, les réseaux futurs intégreront *IntServ* probablement dans l'accès et *DiffServ* dans la dorsale. Une garantie de la QdS est primordiale pour des applications en temps réel et commerciales telle que la téléphonie sur IP, le multimédia et la vidéo en ligne.

2.3.2 Le protocole IntServ (avec RSVP)

IntServ définit les trois classes de services suivantes :

- Garantie : cette classe spécifie et garantit un délai maximal, un seuil de gigue et un niveau assuré de largeur de bande. Ce service est destiné aux applications nécessitant des flots en temps réel.
- Charge contrôlée ou prédictive : cette classe offre un niveau de service constant. Ce service est destiné aux applications impliquant des flots en temps réel mais qui sont capables d'ajuster la quantité de données au niveau de service offert.
- Best-effort.

Au niveau de chaque routeur, trois files de sortie sont prévues pour chaque session pour assurer les trois classes de service. Des mécanismes de contrôle appropriés tels que *Token bucket filter*, WFQ (*Weighted fair queuing*), RED (*Random early detection*) sont utilisés pour assurer les besoins en qualité de service de chaque classe. Les ressources requises en terme de largeur de bande de transmission et de capacité de tampons sont réservées avant de commencer la transmission d'un flux de paquet à l'aide du protocole RSVP.

- **RSVP**

Resource ReSerVation Protocol est un protocole de signalisation utilisé pour réserver de ressources pour des flots de paquets *unicast* et *multicast* dans l'Internet. C'est un protocole simplexe orienté récepteur, car la réservation de ressources est

requise par le récepteur, pour chaque flot de données, les ressources sont réservées de façon indépendante. La signalisation RSVP configure le mécanisme de gestion de la QdS du flot de données à l'intérieur des routeurs supportant RSVP le long du chemin du flot de trafic. Les messages RSVP sont les suivants : *path, reservation, error, reservation confirmation et teardown.* Les messages les plus importants sont *path* et *reservation* (ou *resv*). Chaque message RSVP est composé d'une entête commune et d'un nombre variable d'objets. Chaque message RSVP transporte un objet SESSION. L'objet SESSION contient l'adresse IP de destination du flot, l'identificateur du protocole et le numéro du port de destination. Chaque source de données envoie périodiquement un message *path* qui initialise l'état du chemin au niveau des routeurs le long du chemin allant de l'émetteur vers les destinataires et chaque récepteur transmet périodiquement un message *resv* qui initialise l'état de la réservation au niveau des routeurs le long du chemin inverse allant du destinataire vers l'émetteur. Un message *path* contient les objets suivants :

- SENDER_TEMPLATE : permet d'identifier l'émetteur et consiste en l'adresse IP de l'émetteur et du numéro de port de la source.
- SENDER_TSPEC : décrit les caractéristiques du trafic du flot de données généré par l'émetteur.
- ADSPEC : décrit les caractéristiques des agrégats de QdS du chemin.
- PHOP (RSVP_HOP) : identifie le hop précédent qui a transmis ce message *path.*
- SESSION : identifie la destination du flot

Dans l'état du chemin, un routeur enregistre tous ces quatre objets pour chaque émetteur. Il génère périodiquement les messages *path* et les dirige vers la destination du flot de paquets. Un message *resv* est composé des objets, le FLOW_SPEC et le FILTER_SPEC. Un objet FLOW_SPEC consiste en deux ensembles de paramètres numériques : un RSPEC qui définit la QdS désirée et un TSPEC qui décrit les caractéristiques du trafic du flot de données. L'objet FILTER_SPEC définit un sous-ensemble de paquets devant recevoir la QdS désirée définie dans le RSPEC. L'ensemble

des émetteurs vers lesquels une requête de réservation particulière devrait être transmise pour les différents styles de réservation est décrit par les objets FILTER_SPEC et SCOPE à l'intérieur d'un message *resv*.

Les messages d'erreur RSVP (*PathErr* et *ResvErr*) signalent des erreurs à l'émetteur du message. Le message *PathErr* est envoyé dans la direction *upstream* vers l'émetteur qui a créé l'erreur, tandis que *ResvErr* est transmise au récepteur si la réservation est rejetée au niveau d'un routeur le long du chemin *upstream*. Le message de confirmation de réservation *ResvConf* est transmis au destinataire pour confirmer la requête de réservation. Les messages *Teardown*, *PathTear* et *ResvTear* sont utilisés pour immédiatement retirer respectivement l'état d'un chemin ou d'une réservation. Le *PathTear* est envoyé dans la direction *downstream*, tandis que le *ResvTear* est transmis dans la direction *upstream*.

Le protocole RSVP contient d'autres particularités dont les plus importantes sont l'état de la réservation (*soft state*), la réparation locale (*local repair*) et la fusion (*merging*). RSVP utilise le mécanisme du *soft state* pour contrôler la réservation à l'intérieur des routeurs et des hôtes. Les états *soft state* sont rafraîchis périodiquement par les messages *path* et *resv*. La réparation locale permet une adaptation rapide aux changements du routage. La fonctionnalité de fusion est utilisée pour réduire la signalisation dans la transmission des requêtes de réservation allant de tous les hops suivants vers le hop précédent.

RSVP n'est pas un protocole de routage et il est indépendant du protocole de routage appliqué. Une coordination entre les décisions de routage et la réservation de ressource est indispensable pour un usage efficient des ressources du réseau, de telle sorte que le choix de la route peut dépendre de la qualité du service requis.

Le modèle architectural *IntServ* permet au réseau de garantir un niveau d'exactitude plus élevé et un niveau de granularité plus fin en se basant sur la réservation de ressource prédéterminée pour satisfaire les requêtes de service. La performance de la transmission du routeur peut être dégradée par les mécanismes d'ordonnancement et de

classification des paquets censés fournir des services de type *Differentiated Services* aux flots de données avec ressource réservée.

Comme RSVP a été à l'origine conçu pour des réseaux filaires, de nombreuses anomalies apparaissent lorsqu'il est utilisé pour offrir de la QdS dans des réseaux mobiles [7], [10], [12], [22]. Le premier problème est que RSVP ne possède aucune information sur la mobilité des MNs. Ainsi, lorsque le MN se déplace dans un réseau étranger, le chemin de réservation initial ne sera pas rompu jusqu'au timeout (soft state) et que le nœud effectue la nouvelle réservation par la procédure conventionnelle RSVP. Selon les ressources du réseau, le nouveau chemin n'est pas garanti d'obtenir la QdS requise pour des services temps réel. De plus, étant donné que les réservations initiales occupent toujours des ressources jusqu'à ce qu'elles expirent, de nouvelles requêtes peuvent être bloquées à cause du manque de ressources. Le second problème qui affecte la réservation de la QdS est le "routage triangulaire" dans les réseaux *Mobile IP*. Ce routage triangulaire fait que RSVP réserve sur un chemin inapproprié. Finalement, avant de transmettre des données temps réel, le nœud récepteur doit initialiser un chemin de réservation vers le nœud émetteur. Lorsque le récepteur se déplace vers une nouvelle cellule, il se doit de rétablir le chemin de réservation par la procédure RSVP standard. Cette procédure peut prendre un temps plus long et, en raison de la construction du nouveau chemin de QdS, des connexions temps réel peuvent s'interrompre lors de la relève.

L'intégration de RSVP à la mobilité IP demeure encore un champ de recherche fécond. Actuellement, *IntServ* ne peut être migré dans les réseaux dorsaux IP de grande échelle en raison des problèmes d'évolutivité et de facturation. *IntServ* ne peut supporter des réservations indépendantes de la mobilité.

2.4 Solutions de QdS dans un réseau Mobile IPv6

Dans un environnement IP mobile, les services temps réel nécessitent un bon mécanisme de gestion de la mobilité et de la QdS. Plusieurs solutions adressant la

gestion de la réservation de ressources pour des hôtes mobiles ont été proposées. Ces solutions peuvent être classées selon les mécanismes suivants :

- la réservation par anticipation ;
- l'extension du protocole IPV6 mobile avec l'option du *QOS OBJECT* ;
- la combinaison de MIPv6 et de RSVP.

2.4.1 La réservation par anticipation

La réservation de ressources est indispensable pour garantir de la QdS aux applications d'hôtes mobiles. Plusieurs propositions ont été faites dans le but de réaliser de la réservation par anticipation. L'un des défis majeurs de tels mécanismes est de pouvoir prédire les déplacements du nœud mobile de façon à ce que la réservation par anticipation soit faite à l'intérieur de certaines des nouvelles cellules potentielles. Talukdar et al. [13] ont proposé le protocole de signalisation MRSVP (*Mobile RSVP*) présenté à la Figure 2.15, qui est une extension de l'architecture de réservation de ressources (*IntServ*) permettant à un hôte mobile de faire de la réservation par anticipation le long des chemins de flots de trafic et à partir des cellules ou zones qu'il est probable de visiter durant sa durée de vie de connexion. En effet, avec MRSVP, un nœud mobile peut faire de la réservation de ressources à partir d'un ensemble de cellules ou zones, appelées *MSPEC* (Mobile SPECification). Pour un usage approprié et efficient des ressources, un nœud mobile fera une réservation active à sa position courante mais également des réservations passives à chacune de ces positions appartenant au *MSPEC*. Les réservations passives peuvent être utilisées par d'autres usagers mobiles tandis que les réservations actives appartiennent uniquement à l'usager mobile. Bien que cette proposition résolve le problème du délai mis pour le rétablissement de la QdS, elle présente plusieurs inconvénients. Premièrement, le protocole RSVP doit être modifié considérablement pour supporter les réservations passives. L'introduction d'agents *proxies* avec leur protocole de communication augmente la complexité du réseau. Le modèle de réservation passive et active résulte en un protocole complexe d'une part car

les agents *proxies* de base doivent sauvegarder l'état d'un trop grand nombre d'informations et coûteux d'autre part à cause du gaspillage des ressources et d'un taux de blocage élevé.

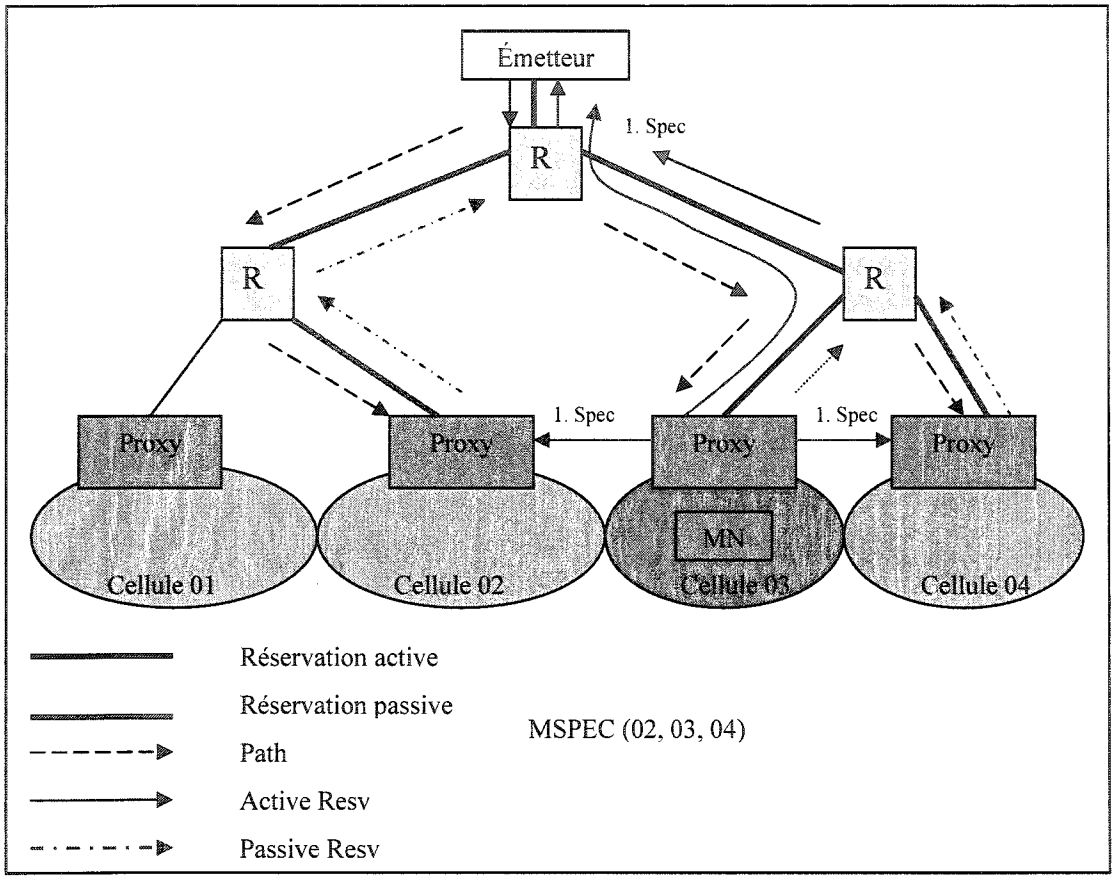


Figure 2.15 Protocole MRSVP

Finalement, un autre problème de MRSVP est qu'il repose sur le nœud MN qui demande sa spécification de mobilité MSPEC.

Tseng et al. [18], dans le but d'améliorer les réservations excessives de MRSVP, ont proposés *Hierarchical MRSVP*. Selon HMRSVP, les ressources sont réservées uniquement lorsque le MN réside dans une zone de chevauchement de cellules frontières de deux régions distinctes. Bien que cette proposition améliore MRSVP en terme de probabilités de blocage, d'interruption forcée, de compléter une session de réservation

tout en fournissant la même QdS, elle ne se débarrasse pas des inconvénients introduits par MRSVP.

2.4.2 L'option de QOS OBJECT

Chaskar et al. [23] ont introduit une nouvelle option d'entête de paquet IPv6 (*HOP BY HOP*), nommée *QOS OBJECT OPTION*, composée d'un ou de plusieurs objets de QdS, pour transporter l'information de QdS pour les flots IP entre un MN et ses CN. Cette option peut être incluse dans les messages d'enregistrement MIPv6 tels que les messages BU et les messages d'accusé de réception BU Ack. Étant donné que le BU est transmis aussitôt que la transmission de données provenant de la nouvelle CoA est prête à commencer, l'option de QdS déclenche les actions nécessaires pour initialiser le traitement de la transmission de la QdS le long du nouveau chemin. Xiaoming et al. [11] se sont basés sur l'option de QdS pour développer le mécanisme appelé "QoS-conditionalized Handoff" présenté à la Figure 2.16. Ainsi, lorsque le MN à la Figure 2.16 effectue un *handover* du routeur d'accès AR1 vers le routeur d'accès AR2, il construit sa nouvelle adresse CoA (newCoA), la réservation de ressource sur le lien montant s'effectue en ajoutant le *QOS OPTION* au message BU tandis que la réservation de ressource sur le lien descendant est faite en ajoutant le *QOS OPTION* au message BU Ack. Par exemple, dans le cas d'une architecture HMIPv6, le temps de latence pour que les paquets reçoivent un traitement de QdS adéquat est considérablement diminué parce que d'une part cette approche ne repose pas sur une signalisation aller-retour telle que Path/Resv de RSVP, d'autre part les messages se dirigent seulement vers l'agent de mobilité régional (MAP) le plus proche. En effet, la transmission bout en bout du *QoS OBJECT* est évitée. Les *QoS OBJECT* peuvent être transmis aussi bien à l'intérieur de n'importe quel paquet IP. Le traitement des objets *QoS OBJECT* aux réseaux intermédiaires est sujet aux mécanismes responsables de la gestion de la QdS du domaine.

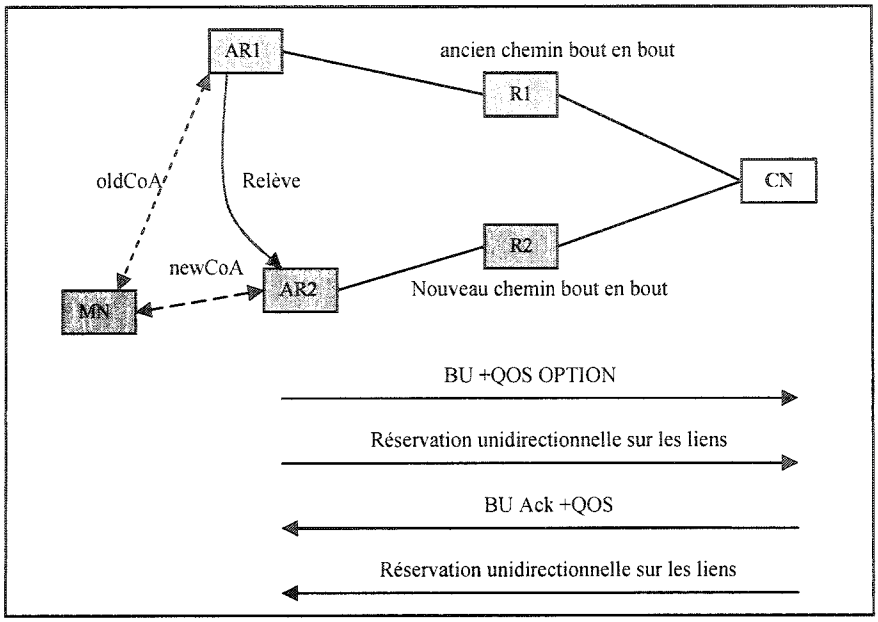


Figure 2.16 Exemple de procédure du QoS-conditionalized Handoff

Cette solution n'a pas créé un profond enthousiasme dans la communauté scientifique surtout pour des raisons de sécurité, car la signalisation de la QdS utilise un mécanisme *in-band* et également parce qu'elle ne permet toutefois aux usagers mobiles de pouvoir sélectionner un autre AR dans le cas de ressources insuffisantes le long de la route entre le MN et le CN. De plus, s'il n'y a pas de messages BU ou de messages BU Ack, il est impossible de mettre à jour la QdS.

2.4.3 Interaction entre MIPv6 et RSVP

Le protocole RSVP est un protocole de signalisation bien mature, plusieurs travaux ont été faits en vue de comprendre l'interaction entre IP mobile et RSVP. Shen et al. [22] ont amélioré RSVP afin de supporter la signalisation pour la QdS dans IP mobile en introduisant un identificateur de flot durant la relève pour l'interaction entre RSVP et IP mobile, en utilisant les avantages de la procédure de RSVP aller-retour (*Path/Resv*) pour initialiser la réservation du nouveau chemin durant les relèves. Terzis et al. [10] ont proposé un mécanisme intégrant un tunnel RSVP avec mobile IP. La Figure 2.17 montre un exemple de tunnel RSVP. Étant donné que le MN est dans son

réseau d'origine, il reçoit continuellement des messages *PATH* provenant du nœud émetteur. Lorsque le MN se déplace à l'intérieur d'une autre cellule, il envoie immédiatement un message BU pour informer le HA de son adresse courante. Ainsi, le HA peut initialiser un tunnel RSVP vers l'agent FA du MN. Le MN peut alors continuer à recevoir les messages PATH après la relève. Lorsque le MN se retrouve distant du HA, le problème du routage triangulaire survient et le chemin de réservation sera long et inefficient.

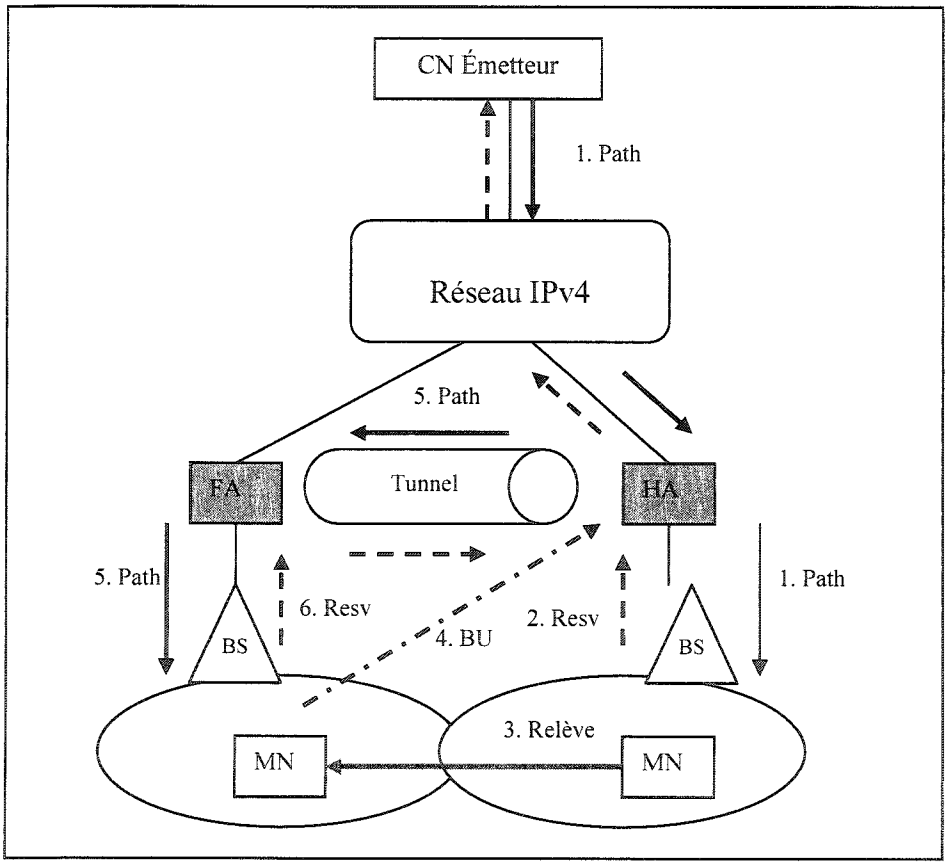


Figure 2.17 Tunnel RSVP avec Mobile IP

Yasukawa et al. [7] ont développé une architecture intégrant RSVP avec Mobile IPv6 proposée afin de réaliser l'optimisation de route pour la transmission de données. La Figure 2.18 présente une vue d'ensemble de l'architecture proposée [7]

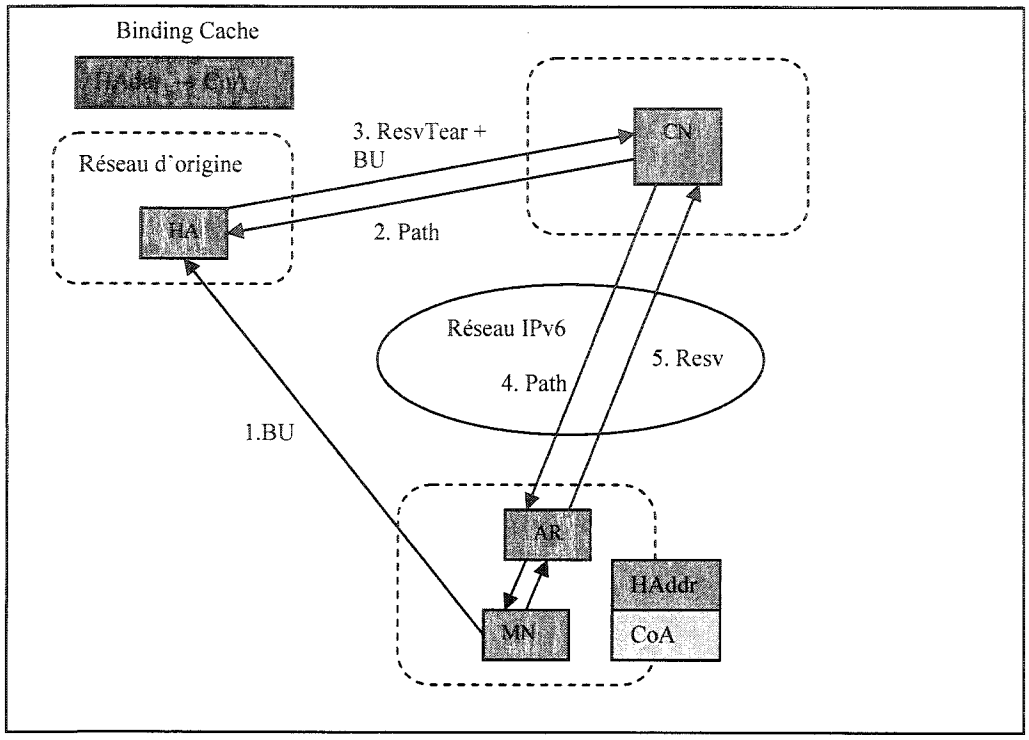


Figure 2.18 Méthode d'optimisation de route utilisant la signalisation RSVP

Procédure pour la méthode d'optimisation de route :

1- Le MN situé dans un réseau visiteur (en dehors de son réseau d'origine) envoie son CoA courant au HA en utilisant le message BU.

2- Le CN qui veut établir une session avec de la QdS envoie un message *Path* au HA (contenant l'adresse Haddr).

3- Lorsque le HA reçoit le message *Path* et note que le MN est hors de son sous-réseau d'origine en regardant sa table de *Binding Cache*, le HA répond au CN en envoyant un message *PathErr*.

4- Sur réception du message *PathErr*, le CN détecte la CoA courante du MN et redirige le message *Path* directement vers le MN.

5- Le MN répond à ce message *Path* avec un message *Resv*.

La Figure 2.19 montre la séquence des messages échangés pour établir la session RSVP.

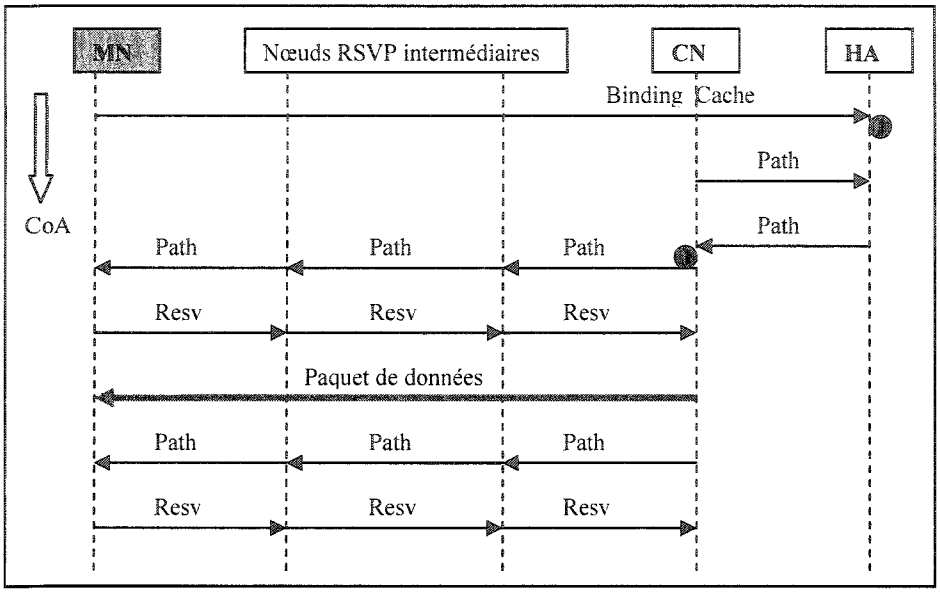


Figure 2.19 Séquence des messages de la méthode d'optimisation de route

La particularité majeure de ce mécanisme est que l'identification du flot (adresses source et destination) repose sur l'adresse CoA du MN. À chaque fois que le MN change de CoA durant une session, une signalisation RSVP de bout en bout entre le MN et le CN est indispensable. Cela résulte en un gaspillage des ressources, une surcharge de la signalisation et un délai élevé de la signalisation de la QdS durant la relève. Le délai de signalisation des requis de QdS, à partir du moment où les paquets utilisant la nouvelle CoA sont émis jusqu'au moment où les mécanismes de gestion de QoS sont configurés le long du nouveau chemin, correspond à un délai aller-retour lorsque le MN est l'émetteur et un délai d'un aller simple lorsque le MN est le récepteur.

Chen et al. [12] ont développé des améliorations à RSVP pour Mobile IP en utilisant le *multicast* et des nouveaux mécanismes de réservation. Comme MRSVP, trois types de réservation sont définis: *RSVP conventionnelle, RSVP prédictive*, et *RSVP temporaire*. D'un autre coté, lorsque le MN se déplace vers une nouvelle cellule, l'agent *proxy mobile* informera les agents *proxies* afin qu'ils rejoignent le groupe *multicast*. De cette façon, le *proxy* mobile dans lequel le MN peut accéder dans le futur recevra un message *Path* et fera une réservation prédictive. L'usage du *multicast* IP devient utile

aux MNs et aux routeurs pour effectuer la réservation de QdS et gérer la mobilité. En d'autres termes, les MNs et routeurs peuvent se joindre à un groupe *multicast* en émettant des messages *IGMP join* [20]. D'autre part, lorsqu'ils veulent retirer la réservation, ils peuvent juste envoyer des messages *IGMP disjoin.* Après avoir quitté le groupe multicast, aucun message *Path* ne sera reçu et les réservations sont interrompues par des opérations *soft-state.* Bien que cette approche minimise la dégradation de service et le délai des paquets et élimine le re-routage des flots de données, les ressources du réseau sont très mal gérées et l'exécution devient plus lourde. Tout compte fait, ces approches combinant RSVP et Mobile IP ont des problèmes d'évolutivité.

2.5 MIPv6 et problèmes ouverts

Le paradigme Qualité de service est un ensemble de requis qu'un système de télécommunications peut offrir lors d'une session. Ces requis peuvent être spécifiés par une application de manière à remplir des facteurs humains ou d'autres facteurs tels que la performance, la fiabilité et la *survivabilité* d'un réseau. Les différents indices de performance généralement rencontrés sont le débit, le délai bout en bout ou aller retour, la gigue, la perte de paquets, liaison unidirectionnelle ou bidirectionnelle, service garanti ou statistique, service inter-domaine ou restreint à un domaine.

Ces dernières années, plusieurs travaux de recherche ont permis de trouver des solutions pour garantir la Qualité de service dans un environnement IP fixe. Des solutions de QdS telles la *Réservation de ressources* (*Integrated Services*) [2] ou la *Priorisation* (*Differentiated Service*) [3] permettent ainsi de garantir les politiques de traitement des paquets de données dépendamment des requis des applications. Lesdites solutions ne sont pas appropriées dans un environnement mobile et un certain nombre de défis restent à relever :

- Délai élevé du rétablissement de la réservation : les messages RSVP doivent traverser deux fois le réseau de bout en bout pour rétablir une session. Ce qui résulte en une détérioration significative de la qualité des flots de données actifs.

- Bande passante limitée : l'utilisation d'une interface radio dans les réseaux mobiles de prochaine génération introduit un problème de disponibilité des ressources au niveau du média radio du fait des requis, en terme de bande de passante, des différentes applications.
- Perte de paquets : le changement de point d'accès durant une communication appelé relève (*Handover ou Handoff*) implique un délai de connexion. Ce délai peut engendrer une perte de paquets critique pour certaines applications temps réels.
- La probabilité de blocage des requêtes de nouvelles sessions : la duplication des requis de ressource dans les environnements à forte mobilité ou dans les réseaux qui supportent un nombre important de nœuds MNs, peut affecter l'efficacité globale du réseau. Dans de tels environnements une nouvelle requête de réservation a une forte probabilité d'être rejetée.
- Trajet sans ressource : la relève entre deux points d'accès différents implique généralement un changement d'adresse. Les flots étant identifiés par l'adresse source et l'adresse destination, un changement d'adresse lors d'une session implique une non réservation au niveau des éléments de réseau et l'utilisation d'une politique de routage par défaut.
- Existence de multitrajets : lors de la relève, plusieurs trajets peuvent être créés dans le but de limiter la perte des paquets de données. La création de multitrajets ne garantit pas la réservation des ressources le long de ces trajets.
- Duplication de réservation de ressources : la relève implique la réservation de ressources le long d'un nouveau trajet. Le relâchement explicite ou implicite des ressources le long de l'ancien trajet peut être rendu difficile du fait, d'une part, de la non connexion avec l'ancien point d'accès et, d'autre part, du fait de la génération de plusieurs messages de rafraîchissement sur l'interface radio.

- Évolutivité : l'explosion exponentielle du nombre d'usagers des systèmes mobiles et de ce fait du nombre de requêtes de QdS pour certaines applications ne permet pas l'intégration de méthodes telles que *Intserv* dans une architecture unifiée de bout en bout.
- Signalisation : le manque de protocole de signalisation dans l'architecture de QdS basée sur *Diffserv* ne permet pas de garantir les services requis par les différentes applications.
- Non-Interopérabilté des architectures de QdS : les différentes architectures ne définissent pas de standard de requête de garantie de service et de ce fait rendent impossible l'intégration de différents mécanismes de QdS (i.e. domaines de QdS hétérogènes : Intserv, Diffserv, MPLS).

CHAPITRE III
MÉCANISME FH-RSVP PROPOSÉ

De plus en plus, les usagers mobiles voudront obtenir les mêmes degrés de satisfaction en matière de qualité de Service (QdS) qu'ils ont sur les réseaux fixes. Ainsi, de nombreuses recherches sont en cours dans le but de résoudre le problème de la qualité de service associée à un flot de trafic dans un environnement mobile, en utilisant le protocole MIPv6 comme protocole de gestion de la mobilité en combinaison avec les protocoles de signalisation de QdS. Dans ce chapitre, nous définissons un mécanisme de réservation de ressources, nommé FH-RSVP. Ce mécanisme devrait permettre en cours de communication de réserver des ressources afin de garantir la QdS sur le nouveau chemin emprunté par les flots de paquets de données échangés entre un MN et son CN après une relève intra-site du nœud mobile. Après avoir formulé quelques hypothèses et concepts de base, nous présenterons l'architecture pour un environnement mobile HMIPv6 intra-domaine, suivi d'une proposition du mécanisme FH-RSVP de qualité de service. Puis, nous ferons une étude comparative détaillée des métriques de QdS. Enfin nous terminerons ce chapitre par une analyse des performances du mécanisme FH-RSVP en terme de probabilités de blocage, d'interruption forcée d'une réservation et de compléter une session de réservation.

3.1 Hypothèses et concepts de base

Le mécanisme *FH-RSVP* de QdS que nous proposerons conservera en grande partie le même format des messages défini dans *RSVPv1* avec comme différence majeure qu'on peut indiquer à quelle entité du réseau sont destinés les messages *Resv* et *Ack*. Ce nouveau mécanisme définit un mode de réservation bidirectionnelle des ressources. Il est orienté émetteur et maintient des états temporaires de réservation de ressources. Il transporte et maintient les paramètres de contrôle de trafic et de contrôle de sécurité. Le mécanisme repose sur l'ensemble des hypothèses suivantes :

- L'architecture utilisée pour développer notre modèle se base sur l'une des propositions de l'IETF pour les réseaux IPv6 mobiles, la structure HMIPv6 (pour *Hierarchical Mobile IPv6*) présentée au chapitre 2 et qui permet de réduire le temps d'enregistrement.
- Le *MAP* est utilisé comme *proxy* de réservation de ressources. À cette fin, il détermine l'acheminement des messages de signalisation de QdS vers l'extérieur ou vers le réseau d'accès. De même, il est capable de déterminer si deux unités mobiles appartiennent au même fournisseur de service et à quel réseau de transport il est relié.
- Au niveau du réseau dorsal, nous supposons que son fonctionnement est transparent à notre mécanisme de QdS et que nous disposons toujours de ressources en quantité suffisante le long des chemins à l'intérieur de ce réseau.
- Au niveau du réseau local du nœud CN, nous considérons que nous avons toujours suffisamment de ressources disponibles sur les liens bidirectionnels lorsque le CN est fixe. Si le CN est mobile il se comportera alors comme un nœud mobile.
- Le mécanisme de relève *Fast-Handoff* proposé par l'IETF [5] et offrant une réduction du temps de résolution d'adresse est utilisé en combinaison avec l'architecture HMIPv6 dans notre modèle de QdS. De plus, notre solution devrait fournir un mécanisme de relève de type *Seamless Handover* (relève sans interruption) sans perte de paquets de données. Cela suppose donc qu'il n'y a pas de perte d'information lorsqu'un nœud mobile passe d'un routeur d'accès à un autre en cours de communication (en mode de transmission ou de réception)
- Les sessions de communications sont initialisées en utilisant *SIP* [19]. *SIP* permet aux unités mobiles de réaliser les associations de sécurité offrant ainsi le routage optimal défini dans MIPv6. De ce fait, le routage triangulaire n'est plus

supporté et chaque unité connaît les adresses (*HAddr*, *RCoA* ou *LCoA)* de l'unité avec laquelle elle communique.

- Une session de QdS *Session_Id* est identifiée de manière unique et permanente durant la communication. Dans [35], il a été proposé d'utiliser l'adresse permanente *HAddr* dans le *Session object* des messages *RSVP* pour identifier une session de QdS.
- Étant donné la complexité que le support *multicast* introduit pour la signalisation de la QdS et le fait que la grande majorité du trafic dans les réseaux IP classiques est un transport *unicast* point à point, nous utiliserons essentiellement des flots de paquets *unicast*. Notre mécanisme de QdS devrait être en mesure par la suite de supporter des flots de paquets *multicast*. FH-RSVP doit supporter des applications en temps réel tel que la voix sur IP.
- Un MAP ou un AR peut réserver des ressources au nom d'un nœud mobile en servant d'agent de QdS (AQdS)

L'architecture et le mécanisme de QdS que nous proposerons utilisent toute la terminologie décrite dans MIPv6, FMIPv6, HMIPv6, et F-HMIPv6. Ils utilisent également les nouveaux termes suivants :

- MN_R (respectivement MN_S) : le nœud mobile est un nœud récepteur (respectivement émetteur) ;
- CN_R (respectivement CN_S) : le nœud correspondant est un nœud récepteur (respectivement émetteur) ;
- MN_RS (respectivement CN_RS) : le nœud MN (respectivement CN) est à la fois émetteur et récepteur ;
- ANx (Access Network) : correspond au réseau d'accès du routeur d'accès x ;
- AQdS : représente l'agent de QdS qui est soit un AR ou un MAP ;
- IR (Intermediate Router): correspond au routeur intermédiaire qui fournit la fonctionnalité de redirection d'un paquet vers une destination donnée;

- NAR : indique le futur routeur d'accès après une relève ;
- PAR : le point d'accès du MN avant la relève ;
- U1 et U2 : indiquent une réservation de ressources dans la direction *Upstream* ;
- D1 et D2: indiquent une réservation de ressources dans le sens *Downstream* ;
- OAR (Overlap Access Router) : c'est un routeur d'accès placé dans la zone ou deux domaines MAP distincts se chevauchent. Le OAR est capable de communiquer ou d'interagir avec les deux MAPs.

3.2 Architecture proposée

Les Figures 3.1 et 3.2 sur lesquelles se basera notre propos montrent l'architecture globale d'un réseau HMIPv6 avec respectivement un nœud CN fixe et un nœud CN mobile.

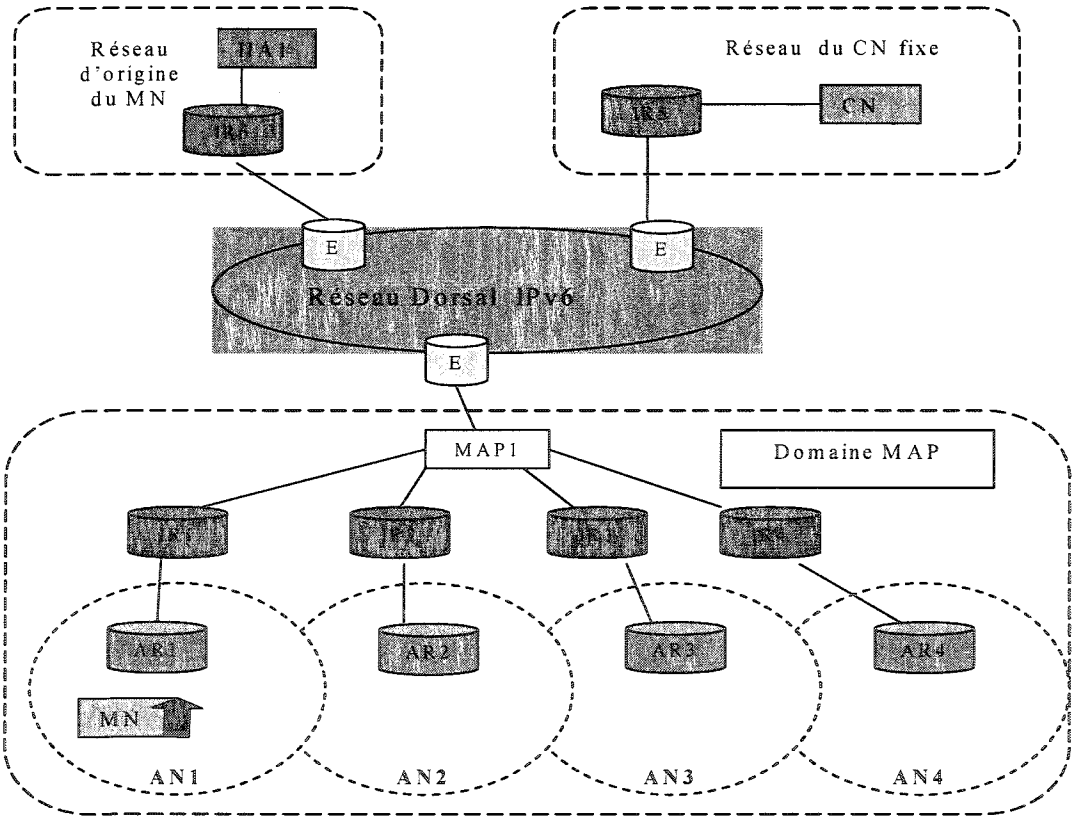


Figure 3.1 Réseau HMIPv6 avec un CN fixe

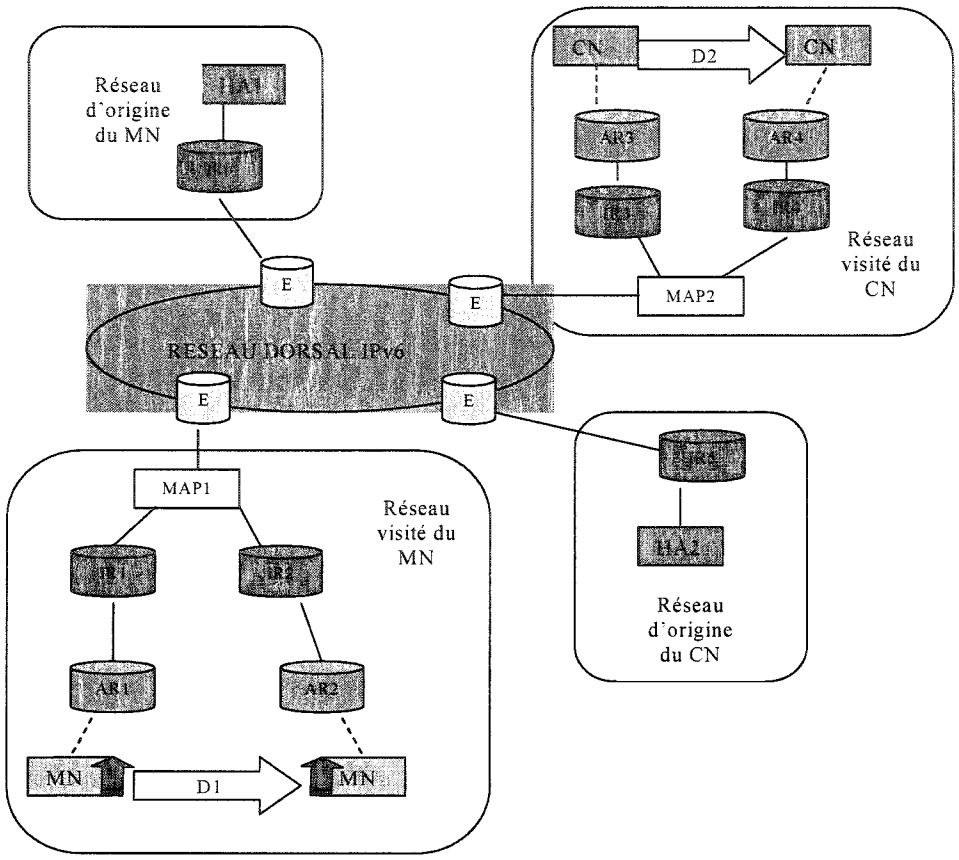


Figure 3.2 Réseau HMIPv6 avec un CN mobile

L'architecture HMIPv6 est composée des éléments suivants:

- le réseau dorsal IPv6 : routeurs IPv6 ;
- le réseau d'origine du MN : HA du MN et routeur(s) IPv6 ;
- les réseaux visités du MN : le(s) MAP(s), le(s) routeur(s) d'accès et le MN ;
- CN stationnaire (Figure 3.1) : routeur(s) IPv6 et le CN ;
- CN mobile (Figure 3.2) : le réseau d'origine et le(s) réseaux visités du CN.

À chaque unité mobile (*MN*) sont associées trois adresses : une adresse permanente (*HAddr),* une adresse temporaire locale (*LCoA)* et une adresse temporaire régionale (*RCoA).* L'unité mobile est soit un émetteur (*MN_S)*, soit un récepteur (*MN_R)*, soit les deux en même temps (*MN_RS*).

À partir de la Figure 3.1 les différents scénarios possibles sont les suivants:

- **Scénario 01 : Le nœud MN est l'émetteur**

Le nœud MN_S émet un flot de données vers le CN_R qui est routeur stationnaire. Pendant l'émission de ce flot de données, le MN_S se déplace d'un routeur d'accès vers un autre routeur d'accès.

- **Scénario 02 : Le nœud MN est le récepteur**

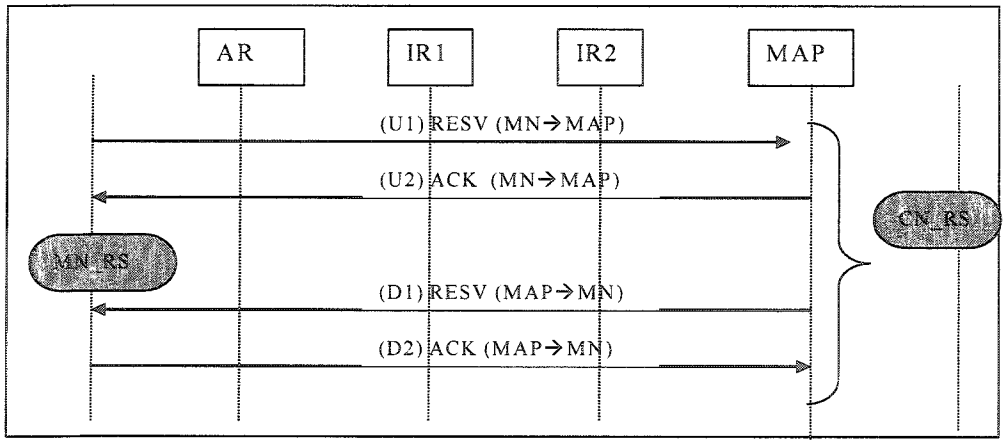
Le nœud CN_S émet un flot de données vers le MN_R. Pendant l'émission de ce flot de données, le MN_R se déplace d'un routeur d'accès vers un autre routeur d'accès.

3.3 Mécanisme FH-RSVP de QdS proposé

Dans cette section, nous décrivons les différentes opérations de notre mécanisme de QdS pour la procédure de réservation initiale et lors de relève en considérant un CN fixe. En effet, un nœud CN mobile se comportera comme un nœud MN.

3.3.1 La procédure de réservation initiale

Pour réserver des ressources avant le début d'une session de communication entre une unité mobile MN et son nœud communiquant, nous utiliserons la procédure de réservation initiale qui va suivre. La Figure 3.3 présente l'ensemble des messages échangés lors de la réservation initiale.



Légende: (U) pour *Upstream* Link et D pour *Downstream* Link

Figure 3.3 Procédure de réservation initiale au réseau local du MN

Le MN et le CN se situant dans des domaines MAPs différents, la réservation initiale entre le nœud MN et le nœud CN se restreint au réseau d'accès du MN. Le MN réserve des ressources sur son lien montant vers le MAP tandis que le MAP qui est l'agent de QdS effectue une réservation au nom du CN pour les ressources sur le lien descendant. Pour ce faire, le *MAP* connaît les requis de QdS du nœud CN. Ces requis peuvent être incorporés lors de l'initialisation de session *SIP* entre les deux entités communicantes. Au niveau du réseau de transport et d'accès distant, les différents paradigmes de réservation implantés restent transparents. Cette approche a pour avantage d'éviter l'initialisation de ressource de bout en bout mais de le faire plutôt de façon locale dans le réseau d'accès du nœud MN. Ainsi, les délais liés à la signalisation de QdS de bout en bout sont évités.

3.3.2 Opérations du mécanisme FH-RSVP lors de la relève du MN

À partir de l'architecture HMIPv6 exposée aux Figures 3.1 et 3.2, nous distinguons uniquement la relève intra-domaine MAP. Ainsi, dans cette section, nous présentons principalement les opérations de notre mécanisme de QdS pour la relève intra-domaine MAP.

- ***Relève intra-domaine MAP***

Nous décrivons ici les opérations génériques dans les cas d'une relève initiée par le mobile. La Figure 3.4 montre la relève intra-domaine MAPs. Nous supposons que l'anticipation de la relève est prise en charge par des mécanismes appropriés de détection (*ou triggers*) de la couche 2, et que les MNs ainsi que les ARs possèdent des fonctionnalités F-HMIPv6.

Le MAP possède l'information nécessaire pour supporter la relève au niveau des ARs situés dans le domaine HMIPv6. Cette information doit inclure l'adresse de la couche liaison (ou identificateur), le préfixe réseau de chaque routeur d'accès et le domaine MAP du point d'accès (DOM_MAP_AP).

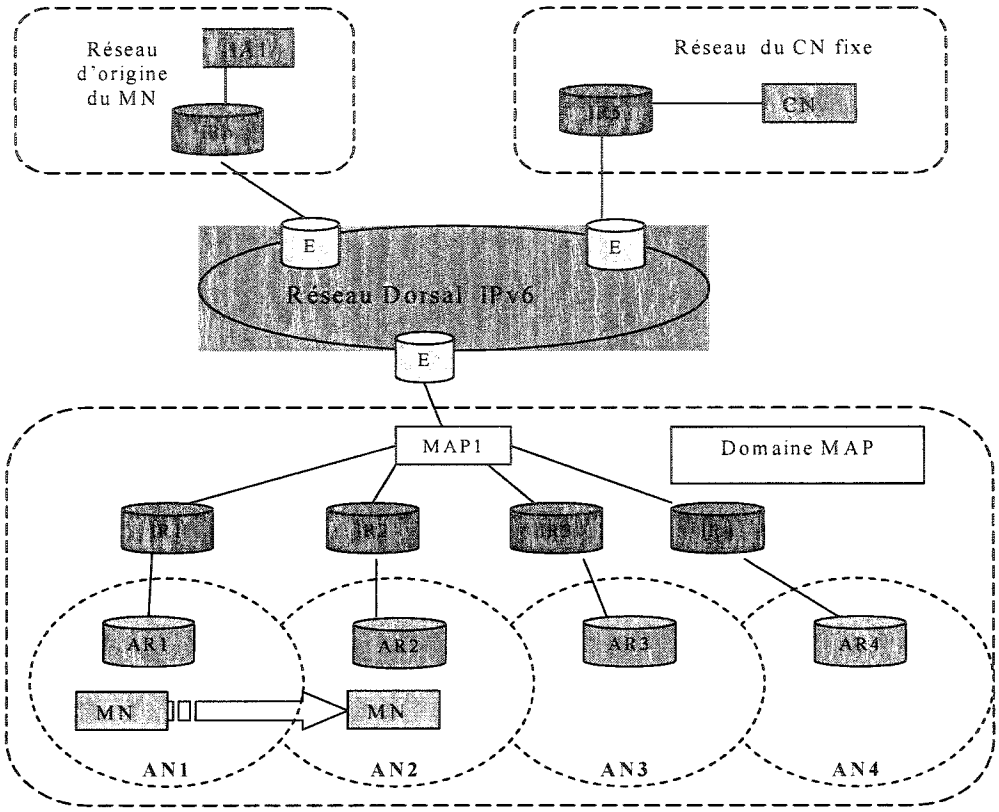


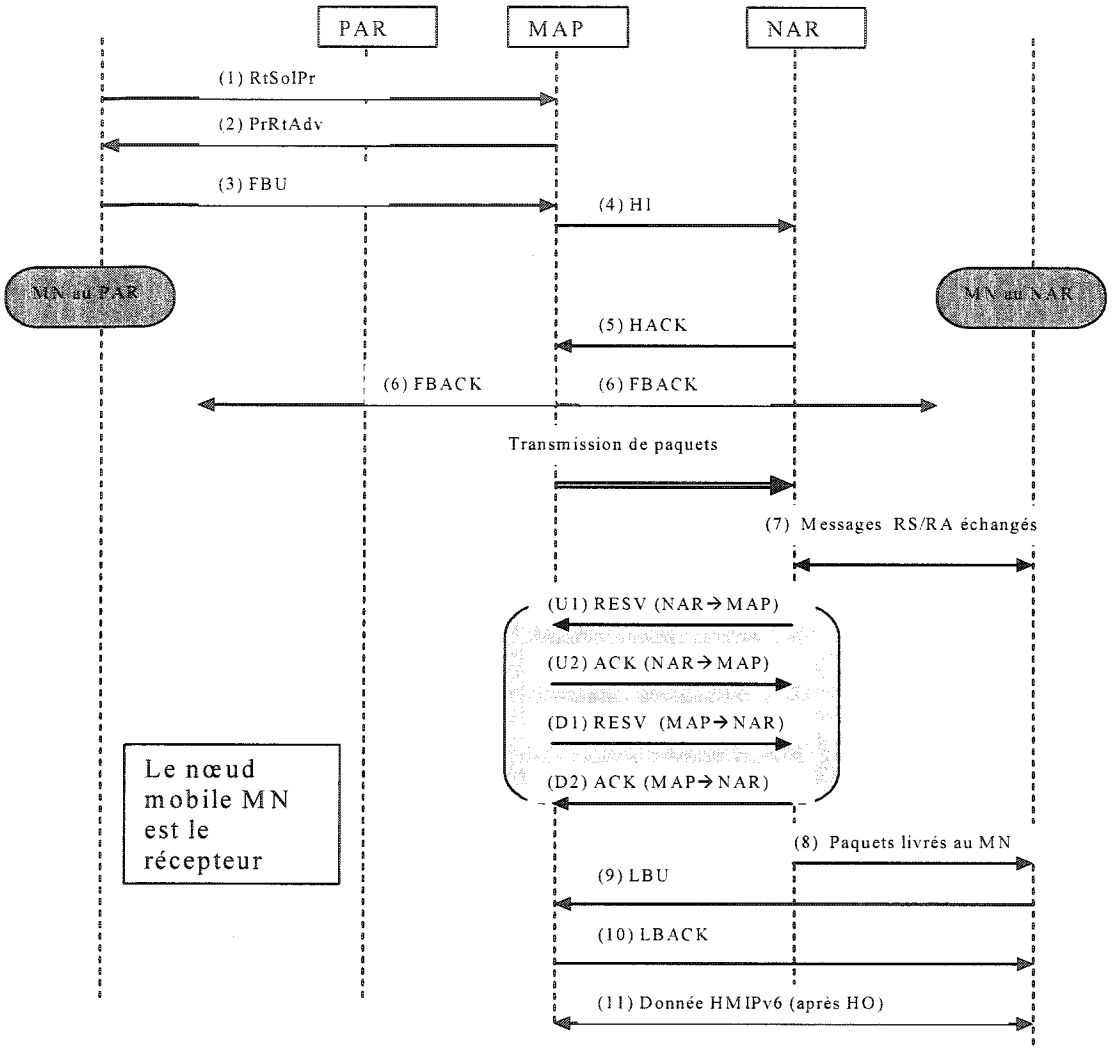
Figure 3.4 Relève intra domaine MAP

- **La relève initiée par le mobile**

Nous décrivons ici les opérations de notre mécanisme pour la relève initiée par le mobile.

- **Basic FH-RSVP (Figure 3.5)**

1. En se basant sur l'anticipation de la relève de niveau 2, le MN envoie un message *RtSolPr* vers son MAP. Le mécanisme de détection (*trigger*) qui permet l'envoi d'un *RtSolPr* peut provenir d'un évènement spécifique à un lien, tel que la promesse d'un signal plus puissant à partir d'un autre point d'accès couplé avec la perte de qualité du signal avec le point d'accès courant. Le *RtSolPr* doit inclure l'information sur l'adresse liaison du lien ou l'identificateur du NAR concerné.



Légende: (U) pour *Upstream Link*, (D) pour *Downstream Link*

Figure 3.5 Basic FH-RSVP pour la relève initiée par le MN

2. Sur réception du *RtSolPr*, le MAP qui administre le PAR (l'ancien routeur d'accès) contient les informations requises sur le NAR (le nouveau routeur d'accès), envoie le message *PrRtAdv* vers le MN qui indique une des conditions possibles suivantes :

A. Si le MAP ne possède aucune entrée correspondant au nouveau point d'attache, il doit répondre en indiquant que le nouveau point d'attache est inconnu. Le MN doit interrompre les opérations du protocole sur le lien courant. Le MN peut envoyer un enregistrement à partir de son nouveau lien.

B. Si le nouveau point d'attache est connecté au PAR lui-même, le MAP doit répondre en indiquant que le point d'attache est connu mais connecté au PAR. Aucune action supplémentaire du protocole n'est nécessaire.

C. Si le nouveau point d'attache est connu et que le MAP possède les informations sur celui-ci, alors le MAP doit répondre en indiquant que le point d'attache est connu. Le message doit contenir l'information sur la *NLCoA* (ou nouvelle LCoA) pour le MN à utiliser dans la région du NAR, i.e. le préfixe réseau des NARs pour une auto-configuration d'adresse de type *stateless* ou la *NLCoA* pour une configuration d'adresse de type *statefull.*

2. Le MN envoie un message FBU au MAP. Le message FBU contient la *PLCoA* et l'adresse IP du NAR.

3. Après la réception du message FBU, le MAP transmettra un message HI vers le NAR afin d'établir un tunnel bidirectionnel.

4. En réponse au message HI, le NAR initialisera une entrée de type *host route entry* pour la *PLCoA* du MN et répondra avec un message HACK.

5. Le MAP envoie des messages FBACK vers le MN en direction du *PLCoA* et du *NLCoA*. Ainsi, le MAP débutera la transmission de paquets de données destinés au MN vers le NAR en utilisant le tunnel établi.

6. Le MN échange des messages *Router Solicitation* (RS) avec le NAR. Le MN arrête d'envoyer des messages RS sur réception d'un message *Router Advertisement* (RA) provenant du NAR indiquant que le MN se trouve uniquement dans la zone d'accès du NAR.

Lorsqu'il détecte qu'il s'est déplacé au niveau radio et qu'il reçoit le RA approprié, le NAR débute alors la réservation bidirectionnelle :

- U1. Le NAR envoie un message RESV vers le MAP afin de réserver des ressources dans la direction *Upstream*.
- U2. Le MAP, sur réception du message RESV, répond avec un message ACK vers le NAR pour confirmer le succès de la réservation de ressources.
- D1. MAP envoie un message RESV vers le NAR afin de réserver des ressources dans la direction *Downstream*.
- D2. Le NAR, sur réception du message RESV, répond avec un message ACK vers le MAP pour confirmer le succès de la réservation de ressources.

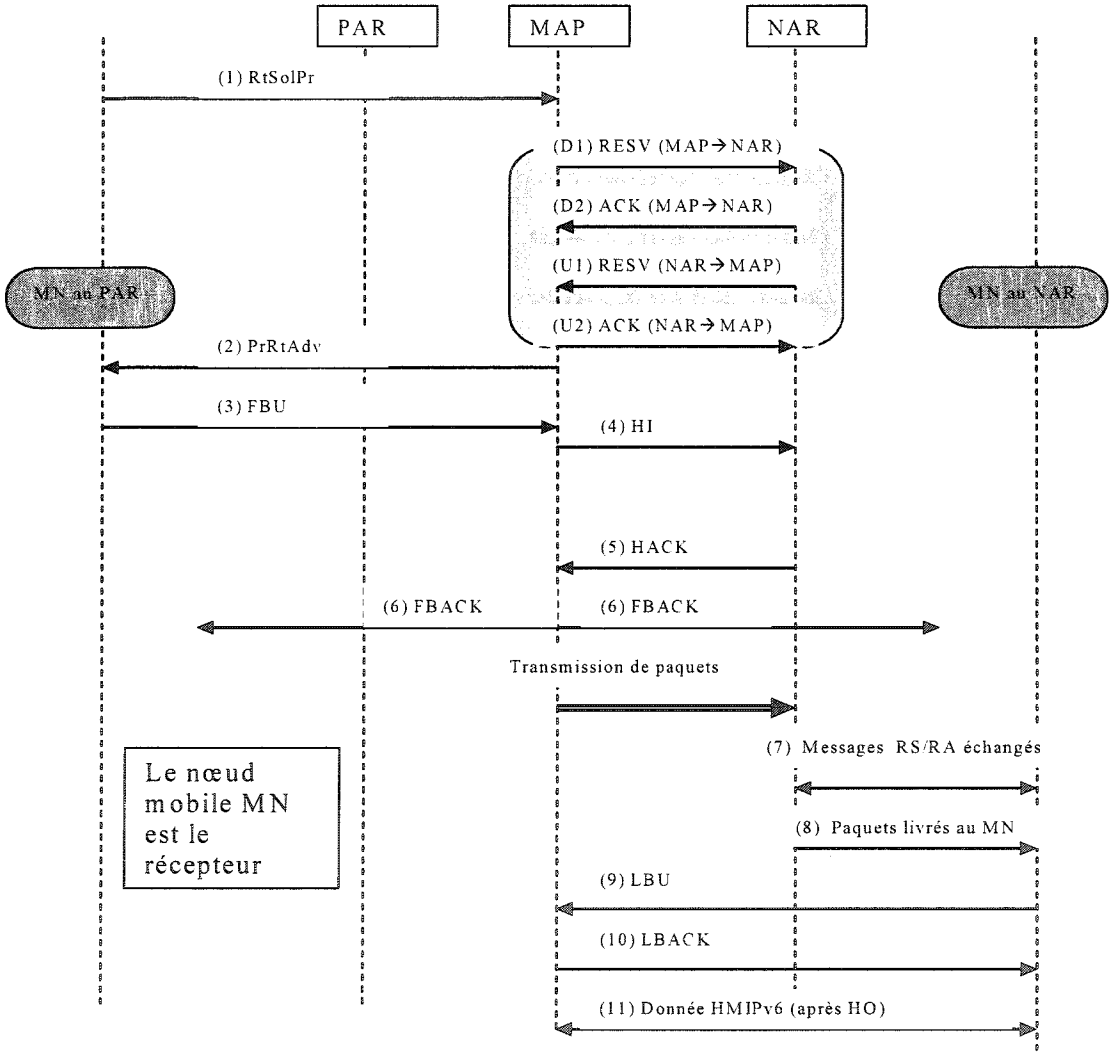
8. Lorsqu'il détecte qu'il s'est déplacé au niveau de la couche 2 et qu'il reçoit le RA approprié, le NAR livre les paquets de données mis en tampon vers le MN à travers la *NLCoA*.
9. Le MN suit alors les opérations normales HMIPv6 en envoyant un LBU au MAP. Lorsque le MAP reçoit le nouveau LBU avec la *NLCoA* provenant du MN, il arrêtera la transmission vers le NAR et annule le tunnel établi pour le *Fast-Handover*.
10. En réponse au LBU, le MAP envoie un LBACK vers le MN et le reste de la procédure suivra la procédure HMIPv6.

- **Fast FH-RSVP (Figure 3.6)**

1. En se basant sur l'anticipation de la relève de niveau 2, le MN envoie un message *RtSolPr* vers son MAP. Le mécanisme de détection (*trigger*) qui permet l'envoi d'un *RtSolPr* peut provenir d'un évènement spécifique à un lien, tel que la promesse d'un signal plus puissant à partir d'un autre point d'accès couplé avec la perte de qualité du signal avec le point d'accès courant. Le *RtSolPr* doit

inclure l'information sur l'adresse liaison du lien ou l'identificateur du NAR concerné.

- Sur réception du *RtSolPr*, si le MAP qui administre le PAR contient les informations requises sur le NAR, le MAP débute alors une réservation bidirectionnelle vers le NAR.



Légende: (U) pour *Upstream Link*, (D) pour *Downstream Link*

Figure 3.6 Fast FH-RSVP pour une relève initiée par le MN

- *Réservation bidirectionnelle*
  - D1. Le MAP envoie un message RESV vers le NAR afin de réserver des ressources dans la direction *Downstream*.
  - D2. Le NAR, sur réception du message RESV, répond avec un message ACK vers le MAP pour confirmer le succès de la réservation de ressources.
  - U1. Le NAR envoie un message RESV vers le MAP afin de réserver des ressources dans la direction *Upstream*.
  - U2. Le MAP, sur réception du message RESV, répond avec un message ACK vers le NAR pour confirmer le succès de la réservation de ressources.

2. Après avoir réalisé la réservation et en réponse au message *RtSolPr* :

- Le MAP qui administre le PAR (l'ancien routeur d'accès) contient les informations requises sur le NAR (le nouveau routeur d'accès), envoie le message *PrRtAdv* vers le MN qui indique une des conditions possibles suivantes :

  A. Si le MAP ne possède aucune entrée correspondant au nouveau point d'attache, il doit répondre en indiquant que le nouveau point d'attache est inconnu. Le MN doit interrompre les opérations du protocole sur le lien courant. Le MN peut envoyer un enregistrement à partir de son nouveau lien.

  B. Si le nouveau point d'attache est connecté au PAR lui-même, le MAP doit répondre en indiquant que le point d'attache est connu mais connecté au PAR. Aucune action supplémentaire du protocole n'est nécessaire.

  C. Si le nouveau point d'attache est connu et que le MAP possède les informations sur celui-ci, alors le MAP doit répondre en indiquant que le point d'attache est connu. Le message doit contenir l'information sur la *NLCoA* (ou nouvelle LCoA) pour le MN à utiliser dans la région du NAR; i.e

le préfixe réseau des NARs pour une auto-configuration d'adresse de type *stateless* ou la *NLCoA* pour une configuration d'adresse de type *statefull.*

3. Le MN envoie un message FBU au MAP. Le message FBU contient la *PLCoA* et l'adresse IP du NAR.
4. Après la réception du message FBU, le MAP transmettra un message HI vers le NAR afin d'établir un tunnel bidirectionnel.
5. En réponse au message HI, le NAR initialisera une entrée de type *host route entry* pour la *PLCoA* du MN et répondra avec un message HACK.
6. Le MAP envoie des messages FBACK vers le MN en direction du *PLCoA* et du *NLCoA*. Ainsi, le MAP débutera la transmission de paquets de données destinés au MN vers le NR en utilisant le tunnel établi.
7. Le MN échange des messages RS et RA avec le NAR.
8. Lorsqu'il détecte qu'il s'est déplacé au niveau de la couche 2 et qu'il reçoit le RA approprié, le NAR livre les paquets de données mis en tampon vers le MN à travers la *NLCoA*.
9. Le MN suit alors les opérations normales HMIPv6 en envoyant un LBU au MAP. Lorsque le MAP reçoit le nouveau LBU avec la *NLCoA* provenant du MN, il arrêtera la transmission vers le NAR et annule le tunnel établi pour le *Fast-Handover.*
10. En réponse au LBU, le MAP envoie un LBACK vers le MN et le reste de la procédure suivra la procédure HMIPv6.

3.4 Analyse détaillée des éléments du mécanisme FH-RSVP

Dans cette section, nous effectuons d'abord une analyse mathématique du délai de bout en bout d'un paquet, du délai de mise à jour du chemin de QdS, du nombre de

paquets reçus, rejetés et perdus lors d'une session de communication, puis une analyse sur le débit de l'application.

3.4.1 Estimation du délai bout en bout d'un paquet

L'équation (3.1) présente le délai de bout en bout d'un paquet allant d'un nœud source (nœud CN) vers le nœud destinataire (nœud MN).

Soit D le délai de bout en bout donné par l'équation suivante :

$$D = D1 + D2 + D3 + D4 \qquad (3.1)$$

où

- D1 est le délai de transmission ;
- D2 est le délai du lien ;
- D3 est le délai de traitement des nœuds ;
- D4 le délai de mise à jour du chemin de QdS.

Le délai (D4) de mise à jour du chemin de QdS apparaît lorsqu'un nœud MN s'apprête à faire une relève.

Soit les paramètres suivants:

$D_f(x, y)$: distance d'un lien filaire reliant le nœud x au nœud y

$L_f(x, y)$: lien filaire reliant le nœud x au nœud y

$L_r(x, y)$: lien radio reliant le nœud x au nœud y

T1 (x, y) : délai de transmission d'un lien filaire $L_f(x, y)$

Id (x, y) : délai de transmission de l'Internet dans le réseau dorsal IPv6 d'un lien filaire $L_f(x, y)$ appartenant au réseau dorsal.

T2 (n) : délai de traitement à un nœud n

T3 (x, y) : délai de transmission d'un lien radio $L_r(x, y)$

Taux(x, y): taux de transmission sur le lien $L_f(x, y)$

Taille (p) : taille en bit du paquet p

$$T3(p,(x,y)) = \frac{Taille(p)}{Taux(x,y)} \qquad (3.2)$$

T4 (x, y) : délai de propagation d'un paquet p pour traverser un lien filaire L_f (x, y).

Les signaux électriques dans les câbles filaires coaxiaux voyagent à approximativement deux tiers de la vitesse de la lumière ($V_{Lumière}$ = 3 10^8 m/s). Ainsi, le délai de propagation d'un paquet p pour traverser un lien filaire donné par l'équation (3.3) :

$$T4(x,y) = \frac{3D_f(x,y)}{2V_{lumière}} \qquad (3.3)$$

La Figure 3.7 présente un modèle pour l'étude du délai bout en bout des paquets et du délai de mise à jour de la QdS.

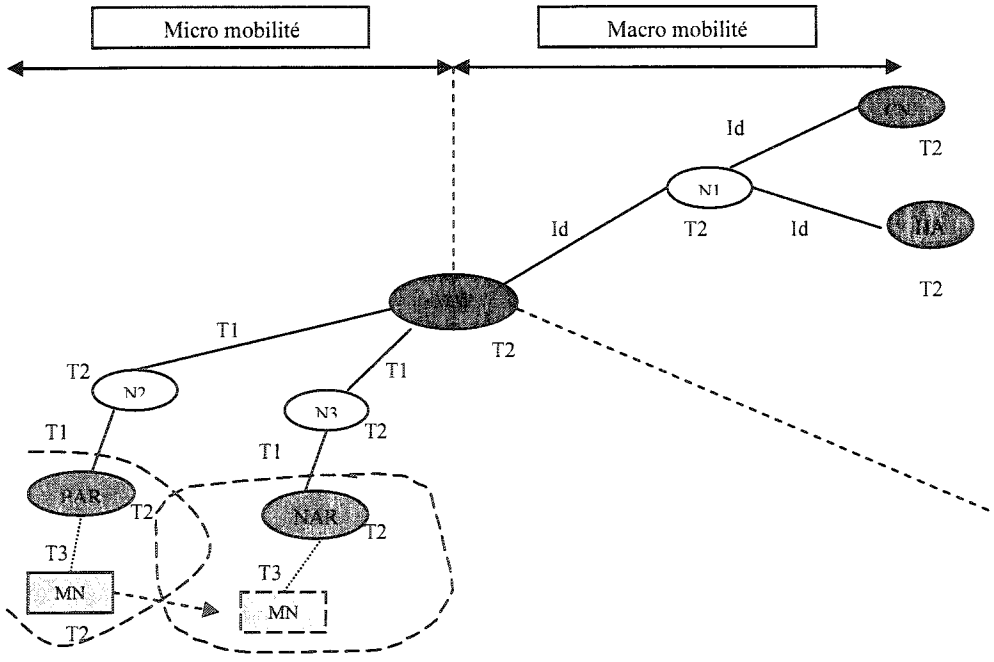


Figure 3.7 Modèle proposé pour l'étude du délai dans un réseau HMIPv6

Afin de simplifier notre analyse, nous négligeons le délai T4 de propagation d'un paquet sur un lien filaire et le délai de traitement T2 à un nœud intermédiaire.

Nous distinguons les paquets p suivants

- paquets temps réels : CBR audio
- paquets de signalisation
- RSVPv2 : RESV, ACK, RESVERR, RESVTEAR
- HMIPv6 et FMIPv6: HI, HACK, RtSolPr, PrRtSol, FBU, FBACK, RS, RA, LBU, LBUACK, BU, BACK

a) Basic FH-RSVP pour une relève intra domaine

Évaluation du délai de bout en bout d'un paquet

- Routage triangulaire (en passant par le HA)

$$D_{RT,\ Basic\ FH\text{-}RSVP} = Id + 2\ Id + Id + T1 + T1 + T3$$

$$D_{RT,\ Basic\ FH\text{-}RSVP} = 4Id + 2\ T1 + T3 \qquad (3.4)$$

- Routage optimal (direct au MAP)

$$D_{RO,\ Basic\ FH\text{-}RSVP} = Id + Id + T1 + T1 + T3$$

$$D_{RO,\ Basic\ FH\text{-}RSVP} = 2Id + 2T1 + T3 \qquad (3.5)$$

Évaluation du délai de mise à jour de la QdS

- Réservation unidirectionnelle

$$D4_{uni,\ Basic\ FH\text{-}RSVP} = 3 * (T3 + 2T1) + 2 * (2T1) + (2T1 + T3) + (N+1) * T3 + 2 * (2T1)$$

$$D4_{uni,\ Basic\ FH\text{-}RSVP} = 16\ T1 + (5+N) * T3 \qquad (3.6)$$

N désigne le nombre de messages RS envoyés par le MN vers le NAR Si N = 1, alors

$$D4 = 16\ T1 + 6\ T3 \qquad (3.7)$$

- Réservation bidirectionnelle

$$D4_{\text{bi, Basic FH-RSVP}} = 3 *(T3 + 2T1) + 2 * (2T1) + (2T1+T3) + (N+1) * T3 + 4 *(2T1)$$

$$D4_{\text{bi, Basic FH-RSVP}} = 20\ T1 + (5 + N) * T3 \quad (3.8)$$

N désigne le nombre de messages RS envoyés par le MN vers le NAR Si N = 1, alors

$$D4_{\text{bi, Basic FH-RSVP}} = 20\ T1 + 6\ T3 \quad (3.9)$$

b) *Fast FH-RSVP pour une relève intra domaine*

Évaluation du délai de bout en bout d'un paquet

- Routage triangulaire (en passant par le HA)

$$D_{\text{RT, Fast FH-RSVP}} = 4Id + 2T1 + T3 \quad (3.10)$$

- Routage optimal (direct au MAP)

$$D_{\text{RO, Fast FH-RSVP}} = 2Id+2T1+T3 \quad (3.11)$$

Évaluation du délai de mise à jour de la QdS

- Réservation unidirectionnelle

$$D4_{\text{uni, Fast FH-RSVP}} = T3 + T1 + T1 + 2 * (T1 + T1)$$

$$D4_{\text{uni, Fast FH-RSVP}} = 6T1 + T3 \quad (3.12)$$

- Réservation bidirectionnelle

$$D4_{\text{bi, Fast FH-RSVP}} = T3 + T1 +T1 + 4 * (T1 + T1)$$

$$D4_{\text{bi, Fast FH-RSVP}} = 10\ T1 + T3 \quad (3.13)$$

c) *Protocole MRSVP*

Évaluation du délai de bout en bout d'un paquet

- Routage triangulaire (en passant par le HA)

$$D_{RT, MRSVP} = 4Id + 2T1 + T3 \quad (3.14)$$

- Routage optimal (direct au MAP)

$$D_{RO, MRSVP} = 2Id+2T1+T3 \quad (3.15)$$

Évaluation du délai de mise à jour de la QdS

Dans le protocole MRSVP, des ressources sont réservées dans la cellule courante du MN, ce sont des ressources dites actives, des ressources sont réservées dans les autres cellules potentiellement visitables et adjacentes à la cellule courante par le MN au cours d'une communication ; ce sont des ressources dites passives. Rappelons d'autre part, que la détection de la relève se fait à l'aide d'un module supportant Mobile IPv4. Une fois la relève détectée, il faut attendre que le MN se retrouve uniquement dans la nouvelle cellule correspondante afin de notifier au module MRSVP qu'il doit activer les ressources passives.

Désignons par TDH le temps entre le moment où la relève est détectée et le moment où le MN se retrouve exclusivement dans la nouvelle cellule. Nous avons :

- Réservation unidirectionnelle

$$D4_{uni, MRSVP} = TDH + T3 + 2T1 + 2\,Id + 3 * (2Id+ 2T1 + T3)$$

$$D4_{uni, MRSVP} = TDH + 8Id + 8T1 + 4T3 \quad (3.16)$$

- Réservation bidirectionnelle

$$D4_{bi, MRSVP} = TDH + T3 + 2T1 + 2Id + 2* 3 * (2Id+ 2T1 +T3)$$

$$D4_{bi, MRSVP} = TDH + 14Id +14T1+ 7T3 \quad (3.17)$$

3.4.2 Perte de paquets

Le nombre de paquets émis au cours d'une session de communication est égal à la somme des paquets reçus, des paquets rejetés et des paquets perdus au cours de ladite session.

Soient

- $P_{transmis}$: le nombre de paquets transmis par le nœud émetteur CN
- $P_{reçus}$: le nombre de paquets reçus par le nœud récepteur MN
- $P_{rejetés}$: le nombre de paquets rejetés aux nœuds intermédiaires ou au nœud MN
- P_{perdus} : le nombre de paquets perdus aux nœuds intermédiaires

Le nombre de paquets perdus devrait vérifier l'équation (3.18) suivante :

$$P_{transmis} = P_{reçus} + P_{rejetés} + P_{perdus} \qquad (3.18)$$

Les nombres de paquets reçus, rejetés et perdus dépendent d'une part des mécanismes de files d'attente implémentés au niveau des différents nœuds et d'autre part des relèves survenant lors de la session de communication et des messages de signalisation.

3.4.3 Débit de l'application

Le débit d'une application dépend du nombre de paquets rejetés et perdus.

Évaluation du débit en cours de session :

Soient

T : la durée de la session de communication

t : l'intervalle de temps au bout duquel est déterminé le nombre de paquets reçus par le nœud récepteur avec $t < T$

Nb_paquets_reçus : le nombre de paquets reçus par le MN pendant l'intervalle de temps t en octet.

$$\text{Débit en cours de session} = \frac{8 \times \text{Nb\_paquets\_recus}}{t \times 1000} \qquad (3.19)$$

Évaluation du débit total moyen :

Soient

T : la durée de la session de communication

Total_Paquets_reçus : nombre total de paquets reçus par le MN au cours de la session de communication en octet.

$$\text{Débit moyen} = \frac{8 \times \text{Total\_Paquets\_recus}}{T \times 1000} \qquad (3.20)$$

3.5 Analyse mathématique

Dans cette section, nous développons un modèle analytique qui nous permettra d'évaluer les performances du mécanisme FH-RSVP en terme de probabilités de blocage, de terminaison forcée d'une session et de compléter une session.

3.5.1 Modèle analytique

Pour réaliser notre modèle analytique, nous utilisons une topologie en grille (*mesh*) X x X pour représenter un environnement mobile avec un nombre illimité de régions. Par exemple, la Figure 3.8 présente un modèle 2-D en grille 8 x 8. Chacune des 8 x 8 cellules (exemple C_{00}) est servie par un routeur d'accès AR_{00} et tous les ARs (X^2) sont administrés à la Figure 3.9 par un routeur *edge* (MAP).

C_{00}	C_{01}	C_{02}	C_{03}	C_{04}	C_{05}	C_{06}	C_{07}
C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}
C_{20}	C_{21}	C_{22}	C_{23}	C_{24}	C_{25}	C_{26}	C_{27}
C_{30}	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}	C_{36}	C_{37}
C_{40}	C_{41}	C_{42}	C_{43}	C_{44}	C_{45}	C_{46}	C_{47}
C_{50}	C_{51}	C_{52}	C_{53}	C_{54}	C_{55}	C_{56}	C_{57}
C_{60}	C_{61}	C_{62}	C_{63}	C_{64}	C_{65}	C_{66}	C_{67}
C_{70}	C_{71}	C_{72}	C_{73}	C_{74}	C_{45}	C_{76}	C_{77}

Figure 3.8 Modèle 2-D en grille 8 x 8

Toutes les cellules sont supposées statistiquement identiques et de même format qui, pour des raisons d'analyse, est considéré comme étant carré avec une longueur L.

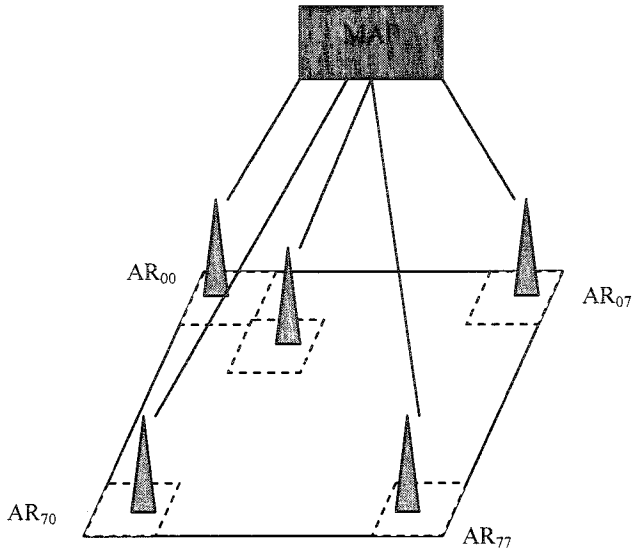


Figure 3.9 Topologie de l'analyse en grille 8 x 8

Pour des raisons de simplicité, les hypothèses suivantes ont été faites :

- Les nœuds mobiles MN se déplacent à une vitesse *v* de façon uniforme le long de la longueur L.
- La répartition des MNs à l'intérieur de chaque cellule est uniforme
- Les nœuds mobiles MN se déplacent à une vitesse *v* de façon uniforme le long de la longueur L.
- Chaque MN peut se déplacer selon les quatre mouvements suivants : vers la gauche, vers la droite, vers le bas et vers le haut (Figure 3.10). D'autre part, lorsqu'un nœud mobile se trouvant dans la cellule C_{00} veut se déplacer vers le haut (respectivement vers la gauche), le MN se retrouve dans la cellule C_{70} (respectivement dans la cellule C_{07}). Il en est de même pour tout nœud mobile qui se trouve dans les autres cellules suivantes C_{07}, C_{70} et C_{77}.

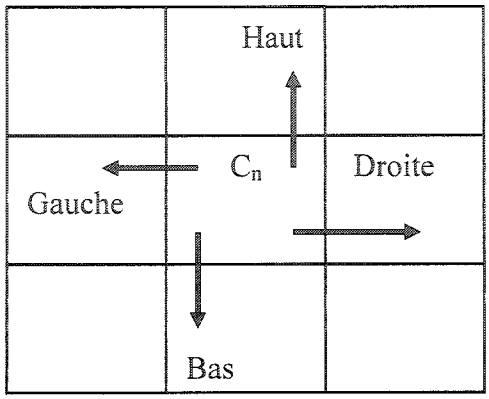


Figure 3.10 Mouvement permis à partir d'une cellule

a) Description des paramètres

Nous allons maintenant définir les paramètres qui seront utilisés dans notre modèle analytique.

- *Temps inter-arrivée de réservation* ($1/\lambda$) : le temps inter-arrivée de réservation représente le temps moyen inter-arrivée de chaque session RSVP d'un MN. Nous supposons que le temps de réservation inter-arrivée est une distribution exponentielle avec pour moyenne $1/\lambda$.
- *Temps de maintenance de réservation* ($1/\mu$): le temps de maintenance de réservation représente le temps moyen de maintenance de chaque session RSVP d'un MN. Nous supposons que le temps de maintenance est une distribution exponentielle avec pour moyenne $1/\mu$.
- *Capacité* (C) : la capacité C représente la moyenne du nombre total de sessions RSVP supporté par une cellule.
- L : la longueur d'une cellule carrée.
- V : la vélocité relative d'un nœud MN dans une cellule.
- *Temps de résidence dans une cellule* ($1/\gamma$) : le temps pendant lequel un appel réside dans une cellule donnée. Nous supposons que le temps de résidence est une distribution exponentielle avec pour moyenne $1/\gamma$ égale à L / V.

- *Nombre moyen de MNs par HA* (n): n représente le nombre moyen de MNs visitant une cellule.
- *Charge fournie* (ρ) : ρ représente la charge fournie par le système pour une cellule et est égale à $n\lambda / C\mu$.
- *Probabilité de blocage de réservation* (P_b) : P_b représente la probabilité qu'un problème apparaisse lorsqu'un MN désire créer une nouvelle réservation pour une session RSVP.
- *Probabilité d'interruption forcée* (P_f) : P_f représente la probabilité qu'une réservation active ne puissent être effectuée avec succès et la réservation est obligée de s'interrompre lorsque le MN effectue une relève vers la nouvelle cellule.
- *Probabilité de compléter une session* (P_c) : P_c représente la probabilité qu'un MN puisse faire une réservation initiale active pour une session RSVP et compléter la session avec succès en regard du nombre de relèves faites par le MN lors du temps de connexion.

b) Calcul des probabilités

- *Probabilité de blocage de réservation* (P_b)

Soient n_C le nombre de canaux disponibles dans une cellule et A la charge offerte dans une cellule. La probabilité de blocage de réservation est donnée par la formule d'Erlang-B suivante :

$$P_b = \frac{\frac{A_c^{n_c}}{n_c!}}{\frac{\sum_{i=0}^{n_c} A^i}{i!}} \qquad (3.21)$$

- *Probabilité d'interruption forcée* (P_f)

Le taux de génération des *handoffs*, λ_h, satisfait l'équation suivante :

$$\lambda_h = P_h \times (\lambda_h + \lambda_o) \times (1 - P_b) \qquad (3.22)$$

L'équation (3.22) est justifiée de la manière suivante : le terme (λ_h + λ_o) désigne le taux total du trafic dû aux nouvelles arrivées (λ_o) et aux relèves (λ_h). En multipliant par (1-P_b) qui est la probabilité que le trafic soit accepté, nous obtenons le taux d'inter-arrivée du trafic actif à l'intérieur de la cellule. Finalement, en multipliant le taux d'inter-arrivée du trafic actif par la probabilité de faire une relève, P_h, on obtient le taux de génération des *handoffs* λ_h dans les cellules voisines.

La probabilité P_h démontrée en annexe (voir section a.1) est donnée également par l'équation:

$$P_h = \frac{1 - e^{-\mu L / V}}{\mu L / V} \tag{3.23}$$

La probabilité d'interruption forcée de réservation est donnée par l'équation suivante :

$$P_f = \frac{(P_h \times P_b)}{(1 - P_h \times (1 - P_b))} \tag{3.24}$$

En remplaçant μL/V par x dans (3.23), nous avons alors :

$$P_h = \frac{(1 - e^{-x})}{x} \tag{3.25}$$

À partir de l'équation (3.25), l'équation (3.26) donne la probabilité P_f:

$$P_f = \frac{\frac{(1 - e^{-x}) \times P_b}{x}}{(1 - \frac{(1 - e^{-x})}{x} \times (1 - P_b))} \tag{3.26}$$

- *Probabilité de compléter une session (P_c)*

La probabilité P_c représente la probabilité qu'un MN établisse une réservation initiale qui n'est pas bloquée pour une session RSVP et que la session RSVP ne soit pas forcée de s'interrompre lors des relèves du MN durant son temps de connexion.

La probabilité Pc est donnée par l'équation 3.27 :

$$P_c = (1 - P_b) \times (1 - P_f) \tag{3.27}$$

Dans le meilleur des cas qui serait de considérer que la probabilité P_f est considérablement petite (i.e. $P_f <<<< 1$), l'équation (3.27) se simplifie pour donner

$$P_c \approx (1 - P_b) \tag{3.28}$$

3.5.2 Estimation des probabilités

Dans cette section, nous allons calculer les probabilités P_b, P_f et P_c dans le cas MRSVP et FH-RSVP. La Figure 3.11 présente la cellule C_{nl} et ses cellules adjacentes C_{gl}, C_{dl}, C_{hl} et C_{bl} (avec g pour gauche, d pour droite, h pour haut et b pour bas).

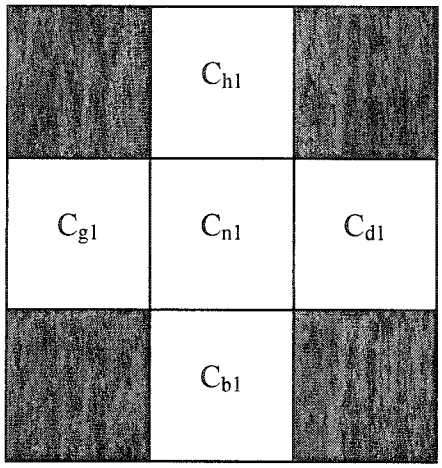


Figure 3.11 Modèle 2-D (à 2 dimensions)

Les différentes probabilités sont calculées en considérant la charge totale réservée à la cellule C_{nl} en tenant compte des nœuds mobiles à l'intérieur des cellules adjacentes C_{gl}, C_{dl}, C_{hl} et C_{bl}.

A. Probabilité de blocage de réservation (Pb)

- MRSVP

La charge initiale offerte réservée par les n nœuds MNs à l'intérieur à la cellule C_{nl} est

$$\rho_{\text{initiale, MRSVP}} = n\lambda/C\mu \tag{3.29}$$

Étant donné que dans MRSVP, des réservations passives sont faites à l'intérieur des cellules adjacentes à la cellule courante du MN, à la Figure 3.12 les n nœuds mobiles

respectivement présents dans les cellules C_{gl}, C_{dl}, C_{hl} et C_{bl} adjacentes à C_{nl} vont respectivement faire à l'avance n réservations passives à l'intérieur de la cellule C_{nl}.
La charge totale offerte passive réservée par les n nœuds MNs respectivement à l'intérieur des cellules C_{gl}, C_{dl}, C_{hl} et C_{bl} est donc donnée par:

$$\rho_{\text{initiale, MRSVP}} = 4 \times n\lambda / C\mu \tag{3.30}$$

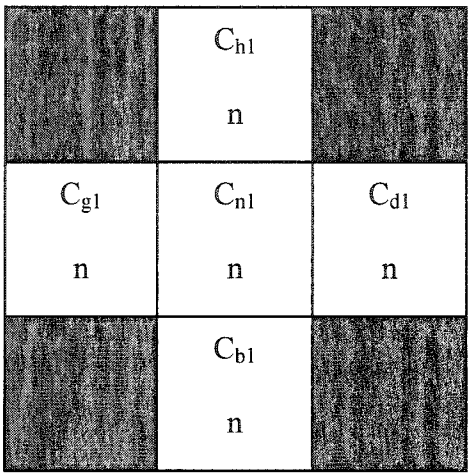


Figure 3.12 Charge totale - protocole MRSVP

La charge offerte totale à l'intérieur de la cellule C_{nl} est donc :

$$\rho_{\text{totale, MRSVP}} = \rho_{\text{initiale, MRSVP}} + \rho_{\text{passive, MRSVP}} \tag{3.31}$$

$$\rho_{\text{initiale, MRSVP}} = 5 \times n\lambda / C\mu \tag{3.32}$$

La probabilité de blocage ($P_{b,\ \text{MRSVP}}$) est obtenue en remplaçant A par $\rho_{\text{totale, MRSVP}}$ dans l'équation (3.21)

- FH-RSVP

Selon l'équation (3.30), la charge initiale offerte réservée par les n nœuds MNs à l'intérieur à la cellule C_{nl} est donc :

$$\rho_{\text{initiale, FH-RSVP}} = n\lambda / C\mu \tag{3.33}$$

Contrairement à MRSVP, dans le mécanisme FH-RSVP, uniquement un sous ensemble des n nœuds mobiles qui appartiennent aux cellules adjacentes C_{g1}, C_{d1}, C_{h1} et C_{b1} et qui effectueront une relève pour se retrouver dans la cellule C_{n1} vont effectivement réserver de manière additionnelle des ressources à l'intérieur de C_{n1} pour garantir la QdS après la relève (Figure 3.13).

Afin de simplifier l'analyse, nous supposons que le nombre de MNs qui effectuent une relève à partir respectivement des cellules adjacentes C_{g1}, C_{d1}, C_{h1} et C_{b1} pour se retrouver à la cellule C_{n1} est équiprobable. Soit β le pourcentage des n nœuds mobiles des cellules adjacentes à C_{n1} qui effectuent une relève pour se retrouver à l'intérieur de la cellule C_{n1}. Le nombre $\beta * n$ correspond donc au nombre de MNs, qui vont faire une relève vers la cellule C_{n1} respectivement à partir des cellules C_{g1}, C_{d1}, C_{h1} et C_{b1}.

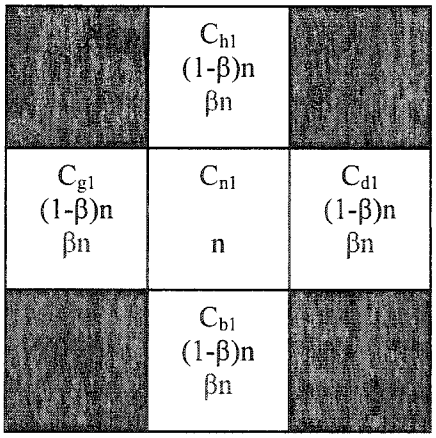


Figure 3.13 Charge totale - FH-RSVP

La charge totale offerte additionnelle réservée par le pourcentage β des n nœuds MN respectivement à l'intérieur des cellules C_{g1}, C_{d1}, C_{h1} et C_{b1} est donc donnée par:

$$\rho_{additionnelle,\ FH\text{-}RSVP} = 4 * \beta\, n\, \lambda / C\, \mu \qquad (3.35)$$

Étant donné qu'une de nos hypothèses précise que les MNs sont uniformément répartis à l'intérieur des cellules, en considérant la cellule C_{n1} le nombre de nœuds mobiles provenant d'une relève des cellules adjacentes C_{g1}, C_{d1}, C_{h1} et C_{b1} ne peut excéder le

nombre de MNs capables de quitter la cellule C_{n1}. Ainsi, nous établissons la condition suivante : $n \geq 4 * \beta n$ d'où $\beta \leq ¼$.

La charge offerte totale à l'intérieur de la cellule C_{n1} est donc :

$$\rho_{totale,\ FH-RSVP} = \rho_{initiale,\ FH-RSVP} + \rho_{additionnelle,\ FH-RSVP} \qquad (3.36)$$

$$\rho_{totale,\ FH-RSVP} = (1 + 4\beta) * n\lambda / C\mu \qquad (3.37)$$

La probabilité de blocage ($P_{b,\ FH-RSVP}$) est obtenue en remplaçant A par $\rho_{totale,\ FH-RSVP}$ dans l'équation (3.21)

B. *Probabilité d'interruption forcée (P_f)*

- MRSVP

La probabilité d'interruption forcée ($P_{f,\ MRSVP}$) est obtenue en remplaçant P_b par ($P_{b,\ MRSVP}$) dans l'équation (3.27). Le terme $P_{h,\ MRSVP}$ est égal à $(1-e^{-\mu L/V})/\mu L/V$ de l'équation (3.23). Il est important de se rappeler que $P_{b,\ MRSVP}$ ne dépend pas du terme β. Nous avons donc:

$$P_{f,\ MRSVP} = \frac{(P_{h,\ MRSVP} \times P_{b,\ MRSVP})}{(1 - P_{h,\ MRSVP} \times (1 - P_{b,\ MRSVP}))} \qquad (3.38)$$

- FH-RSVP

La probabilité d'interruption forcée ($P_{f,\ FH-RSVP}$) est obtenue en remplaçant P_b par ($P_{b,\ FH-RSVP}$) dans l'équation (3.27). Le terme $P_{h,\ MRSVP}$ est égal à $(1-e^{-\mu L/V})/\mu L/V$ de l'équation (3.23). Il est important de se rappeler que $P_{b,\ FH-RSVP}$ dépend également du terme β. Nous avons alors :

$$P_{f,\ FH-RSVP} = \frac{(P_{h,\ FH-RSVP} \times P_{b,\ FH-RSVP})}{(1 - P_{h,\ FH-RSVP} \times (1 - P_{b,\ FH-RSVP}))} \qquad (3.39)$$

C. *Probabilité de compléter une session (P_c)*

- MRSVP

Dans le cas MRSVP, $P_{c,\ MRSVP}$ se calcule en remplaçant P_b et P_f dans l'équation (3.28) respectivement par $P_{b,\ MRSVP}$ et $P_{f,\ MRSVP}$. Nous obtenons alors :

$$P_{c,\ MRSVP} = (1 - P_{b,\ MRSVP}) \times (1 - P_{f,\ MRSVP}) \qquad (3.40)$$

Dans notre étude, les nœuds MN appartenant aux cellules C_{g1}, C_{d1}, C_{h1} et C_{b1} effectueront une unique relève vers la cellule C_{n1}.

- FH-RSVP

Dans le cas FH-RSVP, $P_{c,\ FH\text{-}RSVP}$ se calcule en remplaçant P_b et P_f dans l'équation (3.28) respectivement par $P_{b,\ FH\text{-}RSVP}$ et $P_{f,\ FH\text{-}RSVP}$. Nous obtenons alors :

$$P_{c,\ FH-RSVP} = (1 - P_{b,\ FH-RSVP}) \times (1 - P_{f,\ FH-RSVP}) \qquad (3.41)$$

CHAPITRE IV
IMPLÉMENTATION ET RÉSULTATS

Après avoir présenté le mode de fonctionnement de notre mécanisme FH-RSVP ainsi que les différents paramètres de QdS qui vont permettre d'en évaluer la performance au chapitre précédent, nous procédons dans ce chapitre à l'implémentation de FH-RSVP. Nous débuterons par une description de l'environnement de simulation NS-2 [24] sur lequel notre mécanisme FH-RSVP sera implémenté. Puis, nous présenterons les détails d'implémentations de FH-RSVP. Ensuite, nous proposerons un premier plan d'expérience afin d'évaluer les performances de notre mécanisme de QdS implémenté sur NS-2 par rapport au protocole MRSVP, suivi d'un deuxième plan d'expérience pour comparer FH-RSVP et MRSVP en terme d'utilisation des ressources à l'aide de MATLAB. Nous terminerons ce chapitre par une présentation des résultats correspondants aux deux plans d'expérience, ainsi qu'une analyse détaillée de ceux-ci.

4.1 Environnement d'implémentation et d'expérimentation

Afin de réaliser notre implémentation et d'effectuer nos simulations, nous avons utilisé le simulateur de réseaux NS (*Network Simulator*) dans sa version NS-2.26. Notre choix est motivé essentiellement par le fait que ce simulateur est le plus utilisé pour entreprendre des recherches sur le protocole *Mobile IP* à ce jour et comporte un module *Mobile IPv4*. NS comporte également d'autres protocoles implémentés (ex : TCP, UDP, IP) et propose l'interface graphique NAM (*Network Animator*) pour suivre les échanges de messages. De plus, NS est implémenté en C++ et OTcl, ce qui allie rapidité d'exécution et puissance de calcul. Nous avons donc installé la version *NS-allinone-2.26* sur le système d'exploitation Linux REDHAT 9 utilisant le *GNU gcc 3.22* comme compilateur principal. L'ensemble *NS-allinone* est un *patch* qui contient des composantes requises et certaines composantes optionnelles utilisées pour faire fonctionner NS. Cet ensemble contient un script *"install"* pour la configuration, la

compilation et l'installation automatique de ces composantes. La Figure 4.1 présente l'architecture de base du simulateur NS-2. La version *NS-allinone-2.26* disponible à partir du site officiel de NS [24] comporte les différentes composantes suivantes :

- Tcl release 8.4.5 (composante requise)
- Tk release 8.4.5 (composante requise)
- Otcl release 1.8 (composante requise)
- TclCL release 1.15 (composante requise)
- Ns release 2.26 (composante requise)
- Nam release 1.10 (composante optionnelle)
- Xgraph version 12 (composante optionnelle)
- CWeb version 3.4g (composante optionnelle)
- SGB version 1.0 (composante optionnelle, crée sgblib pour toutes les plates-formes de type UNIX)
- Gt-itm et sgb2ns 1.1 (composante optionnelle)
- Zlib version 1.1.4 (composante optionnelle, mais nécessite l'utilisation de Nam)

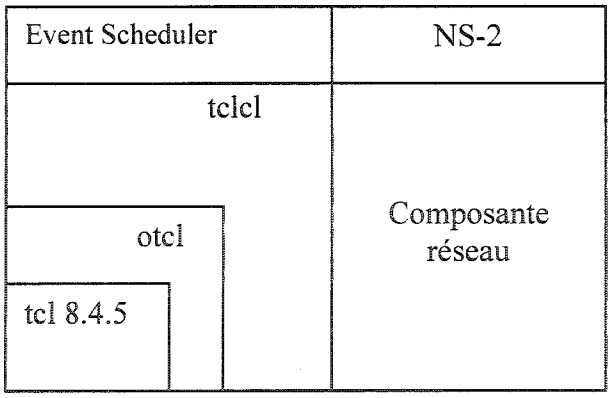


Figure 4.1 Architecture de NS-2

Les détails pratiques concernant la préparation et l'installation complète sont donnés sur le site de NS-2 [24].

Nous utilisons comme matériel un ordinateur processeur Intel Pentium IV CPU 3.01 GHz avec 512 Mo de RAM et 120 Go de mémoire sur le disque dur. Nous avons installé *NS* sur une distribution de linux utilisant un compilateur C++ GNU gcc 3.22.

4.2 Détails d'implémentation

Pour effectuer la réservation de ressources lors de la relève avec le mécanisme FH-RSVP, nous avons développé un module RSVPv2/NS orienté émetteur basé sur le module RSVP/NS [33]. RSVP/NS supporte une réservation orientée récepteur pour des adresses de nœud de type *flat*. Le module RSVPv2/NS devra supporter l'adressage hiérarchique utilisé dans le module Mobile IP de NS-2.

4.2.1 Les Liens RSVPv2

Nous avons implémenté en OTcl un lien nommé *duplex-rsvpv2-links* qui est basé sur le lien *duplex-intserv-links* de NS-2 auquel un objet *RSVPv2Checker* et une file d'attente WFQ sont ajoutés. L'objet *RSVPv2Checker* a pour but d'intercepter les paquets RSVPv2 sur le lien et de les transmettre à l'agent RSVPv2 sur le nœud de destination du lien. Pour envoyer des messages *Resvv2* et *ResvTearv2*, les messages sont contrôlés par l'objet *RSVPv2Checker* d'où le message *Resvv2* provient. Ce dernier initialise l'état du *Resvv2* correspondant. L'entête du paquet pour ces messages est modifiée pour donner l'impression que le paquet provient du *hop* précédent (*previous hop*). Par contre, les messages *ResvErrv2* et *Ackv2* sont transmis d'un hop à un autre hop à partir d'un agent *RSVPv2* vers un agent *RSVPv2*, en utilisant l'information sur le PHOP provenant des états du *Resvv2*. Les messages *Resvv2* doivent être reliés au protocole de routage, étant donné qu'ils doivent être routés à travers les mêmes *hops* que les paquets de données.

Pour la file d'attente, nous utiliserons les algorithmes WFQ et WF^2Q [34] pour permettre les garanties de largeur de bande. Ainsi, RSVPv2/NS ne supporte que le service à charge contrôlée. Les garanties de largeur de bande sont établies par WFQ (ou

WF^2Q) à l'intérieur des liens. Une classe de trafic est assignée à chaque flot de paquet entrant.

4.2.2 Module Mobile IP

Pour recréer un environnement mobile IP, nous avons utilisé la distribution *fhmip NS-extension* [34]. Cette distribution implémente les protocoles suivants comme extension au module Mobile IPv4 de NS-2.26 : *Hierarchical Mobile IPv6, Fast Mobile IPv6, HMIPv6 et FMIPv6 combinés* [29], [31]. La distribution [34] utilise le module *NS-wireless extension* [25], permettant les opérations de base du protocole Mobile IP (v4). Pour le protocole *Hierarchical Mobile IPv6,* un agent *MAP* a été implémenté en [34] afin de fournir les fonctionnalités d'enregistrement du *MAP*. Le MAP supporte uniquement l'utilisation de son adresse comme RCoA pour le MN. Les messages RAs (*Router Advertisements*) ont été modifiés afin d'inclure l'option *MAP advertisement*. D'autre part, les messages de signalisation requis par FMIPv6 tels que *PrRtAdv, PrRtSol, HI, HAck, F-BU, F-BAck, F-NA* sont fournis. Par contre, nous avons ajouté pour le protocole *Mobile IPv6,* une liste de *Binding Cache* au nœud CN afin de fournir les fonctionnalités de routage optimal. Le CN peut utiliser sa liste de *Binding Cache* et fonctionner en mode *Optimized Routing.* Sinon, le CN fonctionne en mode *Triangular Routing* et ne dispose d'une liste *Binding Cache.* Dans ce mode, les paquets émis du CN transitent par le HA et sont redirigés au MN.

4.3 Plan d'expérience pour évaluer FH-RSVP

Cette section commence par élaborer les métriques utilisées pour l'évaluation de performance du mécanisme FH-RSVP. Elle présente la topologie et les conditions du réseau. Elle se termine en explicitant le plan d'expérience.

4.3.1 Métriques de performance

Le but de cette analyse de performance est d'évaluer de façon quantitative les améliorations d'un système utilisant le mécanisme FH-RSVP. Les paramètres qui seront étudiés sont les suivants :

- La largeur de bande par station : permet de mesurer la quantité de paquets de données reçus pendant la simulation par station.
- La perte de paquet : la perte de paquet est définie pour un nœud MN récepteur comme le nombre de paquets perdus durant la relève. Les pertes des paquets sont dans certains cas directement proportionnelles à la latence.
- Le délai de mise à jour de la QdS : le délai de mise à jour de la QdS est défini, pour un MN récepteur, comme le temps encouru entre l'initialisation de la relève par les signaux de déclenchement de niveau 2 (*L2 Trigger*) et la fin des mises à jour des réservations de ressources le long du nouveau chemin pendant la relève avec le mécanisme FH-RSVP.
- La latence de la relève : la latence du *handoff* est définie pour un MN récepteur comme le temps encouru entre le dernier paquet via l'ancienne route et l'arrivée du premier paquet le long du nouveau chemin après la relève. La latence est un paramètre important pour des applications sensibles au délai tel que la vidéo ou la voix sur IP (*VoIP*).

4.3.2 Configuration de réseau

La topologie proposée a été conçue pour être assez grande pour fournir des résultats réalistes tout en étant petite pour être supporté et simulé par NS-2. La Figure 4.2 montre la configuration de réseau qui sera utilisée lors de la simulation. La topologie du réseau HMIPv6 est composée du HA et des nœuds correspondants (CNs) qui sont connectés via l'*Internet* (nœud IR intermédiaire N1) au MAP. Quatre routeurs d'accès (AR1, AR2, AR3 et AR4), représentant chacun un différent sous-réseau IP, sont connectés via trois routeurs IR intermédiaires (N2, N3, N4 et N5) au MAP. Ce réseau

HMIPv6 comporte donc un seul domaine MAP. Les routeurs d'accès sont initialisés à au moins une distance de 450 m les uns des autres avec un espace libre entre eux de 50 m. Cela réduit la complexité d'analyse du résultat, car il existe seulement de l'interférence de signaux. Dans la zone radio, le medium de communication sans fil utilisé est le 2 Mbps Wireless LAN 802.11 [27] fourni par NS-2.26. Dans le domaine de la micro-mobilité, chaque connexion filaire est modélisée par un lien duplex 10 Mbps et 5 Mbps avec un délai de 2 ms. L'Internet qui se connecte au MAP et au HA ou aux CNs est modélisé comme un lien duplex 100 Mbps avec un délai de transmission Internet *Id* par défaut de 25 ms.

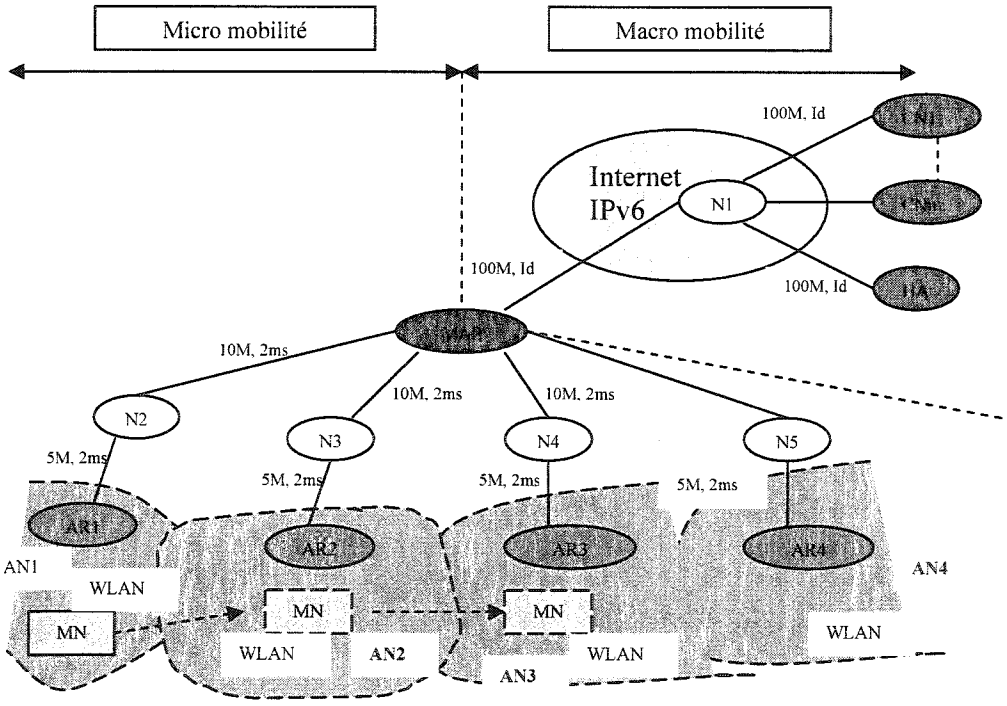


Figure 4.2 Topologie du réseau de simulation

Toutes les caractéristiques des liens filaires et sans fil telles que la largeur de bande (Mbps) et le délai (ms) sont définies à la Figure 4.2. Le nœud mobile MN se déplace dans la zone de couverture selon le modèle RWP (*Random Waypoint Mobility*) [26].

Étant donné que le rayon de couverture de transmission des routeurs d'accès est de 250 m, la zone de couverture totale obtenue à la Figure 4.3 est de 1850 x 500 mètres carrés.

De plus, des agents RSVPv2-NS sont placés à tous les nœuds fixes (CN, N1, N2, N3, N4, N5) et à tous les routeurs d'accès (AR1, AR2, AR3 et AR4) afin de pouvoir y réserver des ressources lors de la session de communication. Avant le début de la session de communication des ressources, et selon certaines hypothèses formulées au chapitre 3, des ressources sont réservées de manière bidirectionnelle sur les chemins suivants : du CN vers le HA, du HA vers le MAP, du CN vers le MAP et du MAP vers le routeur d'accès AR1.

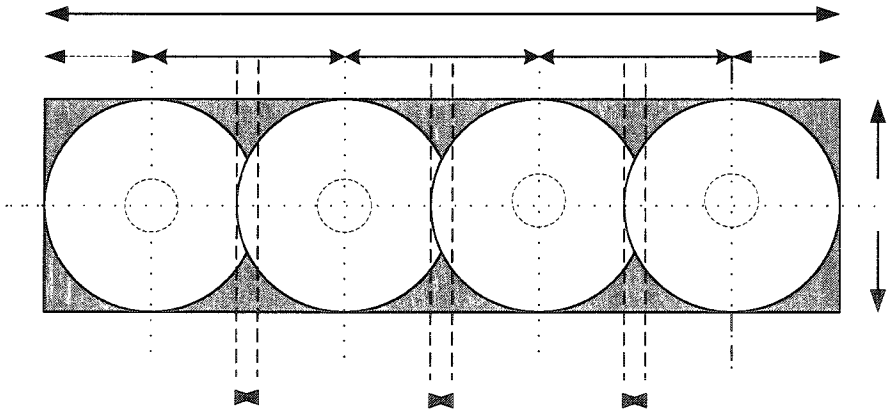


Figure 4.3 Positionnement des routeurs d'accès

Pour simuler un trafic en temps réel, nous créerons un nœud correspondant (CN) comme étant une source de trafic constant (CBR) en utilisant le protocole UDP. Les paquets auront une taille de 200 octets. Un correspondant qui génère un trafic CBR peut être assimilé à un trafic temps réel audio.

4.3.3 Scénarios de la simulation NS-2

Le MN est initialement placé près de son *Home Agent* HA. Au temps t = 6 s, nous déplaçons le MN pour le placer dans le réseau d'accès AN1 du routeur d'accès

AR1. Puis, au temps t = 9 s, nous démarrons la session de communication entre le CN et le MN. Au temps t = 10 s, nous amorçons le mouvement du MN qui se déplace linéairement à une vitesse constante *v* vers le réseau d'accès AN2, ensuite vers le réseau d'accès AN3 et enfin vers le réseau d'accès AN4. Nous distinguons alors deux modes de déplacements : le premier mode est dit *Pause* et le second est dit *Straight.*

A. Le mode Pause

Le mode *Pause* représenté à la Figure 4.4 se décompose de la manière suivante :

1. À t = 10 s, le MN se déplace du routeur AR1 vers le routeur AR2 à une vitesse constante *v.* Le nœud mobile MN marque un temps d'arrêt lorsqu'il atteint la position du routeur d'accès AR2.
2. À t = T1, le MN commence à quitter le routeur AR2 vers le routeur AR3 à la vitesse *v.* Le nœud mobile MN marque un nouveau temps d'arrêt lorsqu'il atteint la position du routeur d'accès AR3.
3. À t = T2, le MN commence à quitter le routeur AR3 vers le routeur AR4 à la même vitesse *v.* Le nœud mobile MN arrête de se déplacer lorsqu'il atteint la position du routeur d'accès AR4.

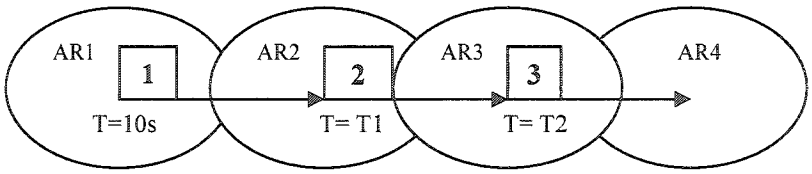


Figure 4.4 Déplacement en mode *Pause*

B. Le mode Straight

Le mode *Straight* présenté à la Figure 4.5, à l'opposé du mode *Pause*, suppose un déplacement direct à partir de t =10 s du nœud mobile MN du routeur AR1 vers le

routeur AR4 en passant successivement par les routeurs d'accès intermédiaires AR2 et AR3 sans marquer de temps d'arrêt.

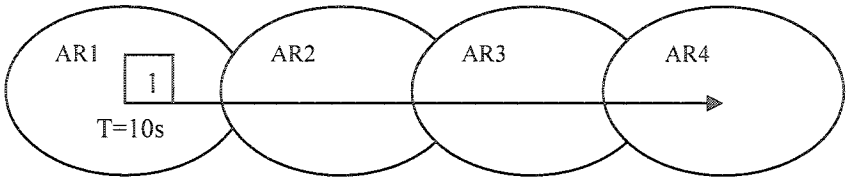


Figure 4.5 Déplacement en mode *Straight*

Le CN arrête de transmettre des paquets à t = *t_sim*. La durée totale d'une simple simulation est de 1380 s et de 330 s. La durée de la session de communication entre le CN et le MN est donc respectivement de 1371 s et de 321 s.

4.3.4 Simulations sous NS-2 et expériences avec MATLAB

Nous présentons dans cette section les simulations à réaliser sous NS-2 et les expériences à faire avec MATLAB.

- *NS-2*

Les facteurs qui semblent influencer appréciablement la valeur des indices de performance définis auparavant sont: la vitesse du MN (*v*), le délai de transmission sur Internet (ld), le débit de paquets provenant du CN (*debit_pqt*). Les zones d'accès étant essentiellement composés de WLAN, la zone de chevauchement n'a pas d'impact majeur sur les métriques de performance.

La vitesse du MN est un facteur pertinent vu que le nombre de paquets perdus pendant la relève en dépend énormément ainsi que la possibilité d'échec d'une relève d'ailleurs (perte de signalisation utilisée pour établir une relève). Nous choisirons les vitesses allant de 1 m/s à 50 m/s et plusieurs vitesses intermédiaires. Le délai de transmission sur Internet (Id) est un facteur important, vu que le délai de mise à jour des HA et CN dépend beaucoup de cette valeur. Nous choisirons les valeurs 10, 25, 50, 75,

100, 125, 150, 175 et 200 ms pour pouvoir représenter une mobilité locale et globale du MN. Le débit de paquets provenant du CN (*debit_pqt*) est un facteur important, vu que le nombre de paquets perdus durant la relève en dépend énormément. Nous choisirons des débits allant de 32, 64, 96, 128, 160 et 192 kbps pour pouvoir couvrir tous les genres de trafics UDP CBR.

Les niveaux de ces facteurs seront choisis de manière à couvrir adéquatement l'étendue de variation de ce facteur. D'un autre coté, nous minimiserons le nombre total de niveaux pour des raisons économiques. Le Tableau 4.1 représente les différents niveaux des facteurs.

Tableau 4.1 Niveaux des facteurs – NS-2

Facteur	**Symbole**	**Niveaux**	**Unité**
Vitesse du MN	*v*	1, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	m/s
Délai de la transmission Internet	Id	10, 25, 50, 75, 100, 125, 150, 175 et 200	ms
Débit de paquets	*debit_pq*	32, 64, 96, 128, 160 et 192	kbps
Premier temps d'arrêt	*T1*	105 et 470	s
Second temps d'arrêt	*T2*	210 et 930	s
Temps de simulation	*t_sim*	330 et 1380	s

Nous ferons un plan d'expérience un facteur à la fois pour mieux remarquer l'influence de chaque facteur sur les indices de performance observés et pour minimiser le nombre d'expériences comparé à une conception factorielle.

- **MATLAB**

Les facteurs qui semblent influencer appréciablement la valeur des probabilités de blocage, d'interruption forcée et de compléter une session sont: la charge totale offerte (ρ), le pourcentage total de MNs (β) provenant des cellules adjacentes qui font un

handoff vers la cellule courante et le terme x qui est égale à μL/V de l'équation (3.4).

La charge totale offerte est un facteur pertinent, vu qu'une augmentation de la charge peut accroître le risque d'avoir des appels bloqués. Nous choisirons une charge offerte allant de 0.1 Erlang à 1 Erlang avec un pas de 0.1.

Le pourcentage total de MNs (β) provenant des cellules adjacentes qui font un *handoff* vers la cellule courante est un facteur important, vu que la charge additionnelle à réserver en dépend. Nous choisirons les valeurs 1%, 2%, 3%, 4%, 5%, 10%, 15%, 20% et 25% pour pouvoir représenter une augmentation du flux de MNs qui pénètrent dans la cellule courante.

Le terme x qui dépend de la vélocité relative du MN permettra donc de représenter les mobilités suivantes : mobilité *indoor*, mobilité piétonne et la haute mobilité. Nous fixons les valeurs de $1/\mu$ et de L respectivement à 120 s et 400 m. Nous choisirons des valeurs de vélocité du MN de 2 km/h (mobilité *indoor*), de 4 km/h (mobilité piétonne) et de 50 km/h (mobilité forte) correspondant respectivement à des valeurs de x égales à 6, 3 et 0.240.

Les niveaux de ces facteurs seront choisis de manière à couvrir adéquatement l'étendue de variation de ce facteur. D'un autre coté, nous minimiserons le nombre total de niveaux pour des raisons économiques. Le Tableau 4.2 représente les différents niveaux des facteurs.

Tableau 4.2 Niveaux des facteurs – MATLAB

Facteur	**Symbole**	**Niveaux**	**Unité**
Charge offerte	ρ	0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0	Erlang
Pourcentage de *handoffs* provenant des cellules adjacentes	β	0.01, 0.02, 0.03, 0.04, 0.05, 0.10, 0.15, 0.20, 0.25	ms
Le terme μL/V	x	6, 3 et 0.24	

Nous ferons un plan d'expérience tenant en compte de la corrélation des facteurs pour mieux comprendre l'influence combinée des différents facteurs sur les indices de performance observés.

4.4 Résultats de simulations et analyse

Dans cette section, nous présentons l'ensemble des résultats obtenus et une analyse détaillée de chacun des résultats.

4.4.1 Paquets rejetés

Les Figures 4.6, 4.7 et 4.8 montrent le nombre de paquets rejetés en fonction respectivement de la vitesse du MN, du débit de l'application et du délai de transmission de l'Internet *Id* pour les quatre scénarios FH-RSVP simulés (Fast FH-RSVP Pause, Basic FH-RSVP Pause, Fast FH-RSVP Straight, Basic FH-RSVP Straight) et MRSVP. De façon générale, les paquets CBR UDP émis à partir du CN vers le MN ont une taille de 200 octets.

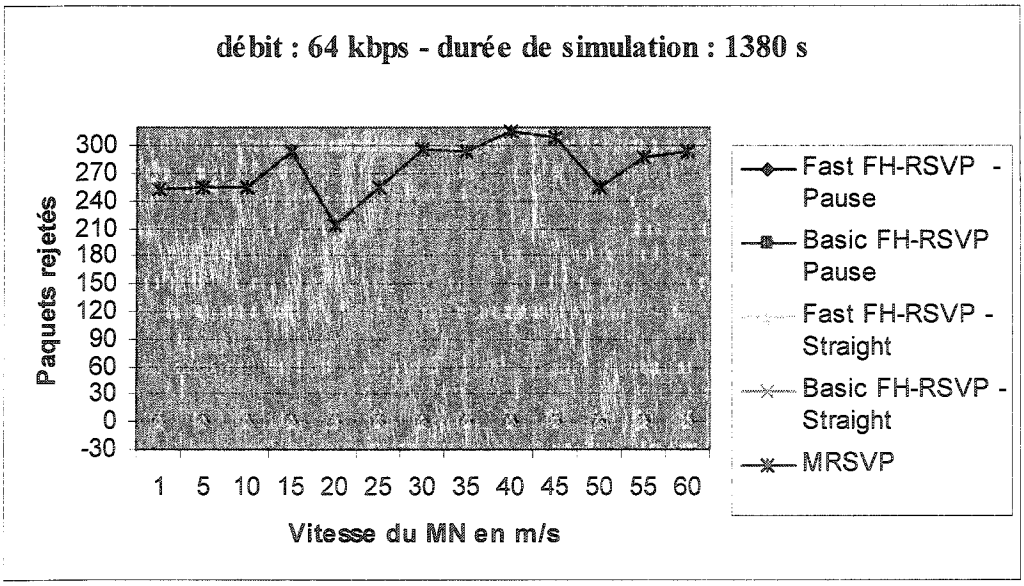


Figure 4.6 Nombre de paquets rejetés en fonction de la vitesse du MN

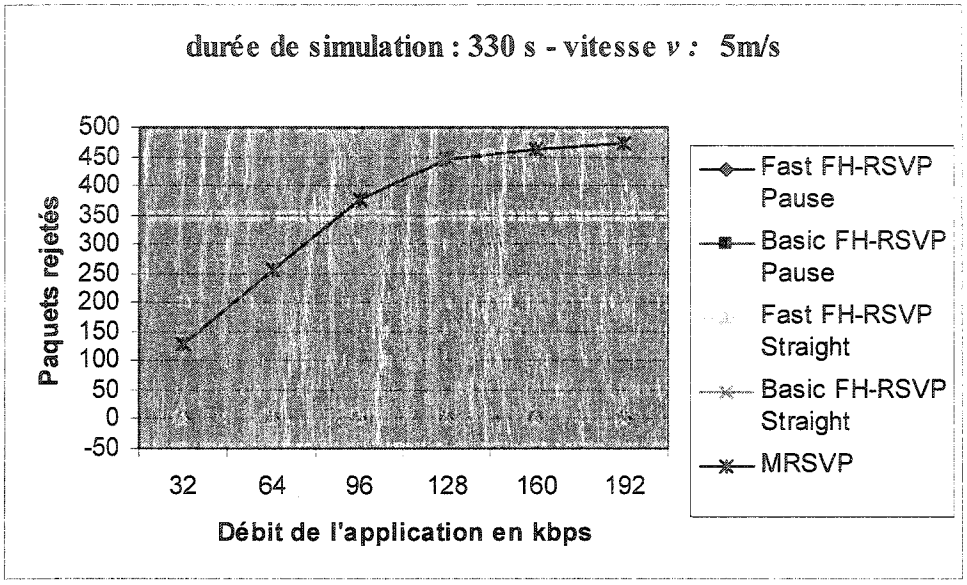


Figure 4.7 Nombre de paquets rejetés en fonction du débit de l'application

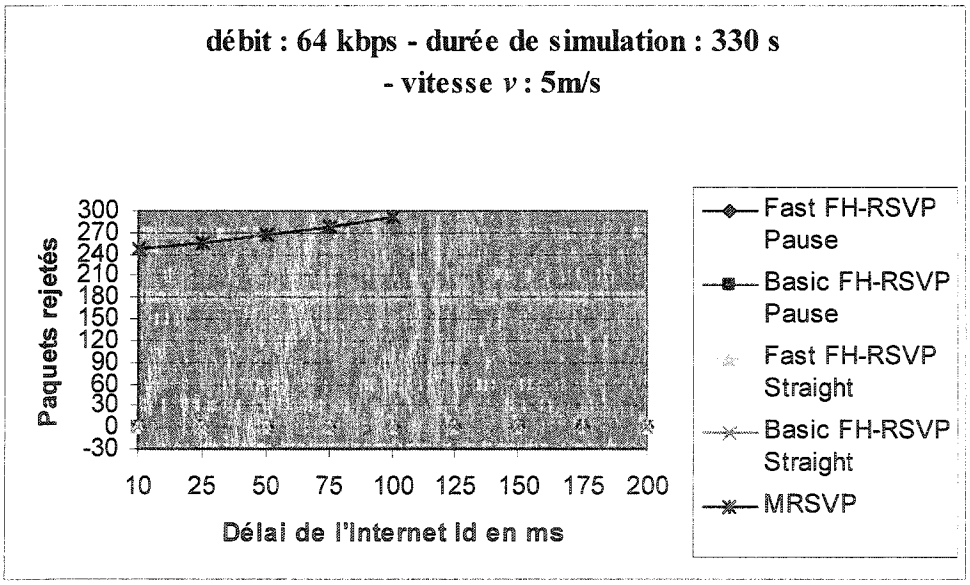


Figure 4.8 Nombre de paquets rejetés en fonction du délai de l'Internet

La durée des 5 scénarios simulés est de 1380 s à la Figure 4.6 et de 330 s aux Figures 4.7 et 4.8. Le débit de transmission des paquets est de 64kbps aux Figures 4.6 et 4.8 tandis qu'il varie selon le facteur *debit_pq* à la Figure 4.7.

En général, nous remarquons que le nombre de paquets rejetés avec MRSVP est toujours plus grand que celui avec FH-RSVP. Ainsi, les Figures 4.6, 4.7 et 4.8 révèlent que pour les quatre scénarios FH-RSVP étudiés, aucun paquet n'a été rejeté. La vitesse du MN qui couvre tous les types de mobilité (*indoor, piétonne et forte*) lorsqu'elle augmente, n'influence pas le nombre de paquets CBR rejetés (Figure 4.8). D'autre part, en augmentant le débit de l'application de 32 à 192 kbps, nous ne remarquons aucun rejet de paquets pour FH-RSVP mais, avec MRSVP qui utilise Mobile IPv4, cela produit une augmentation du nombre de paquets rejetés. Enfin, le délai de transmission de l'Internet à la Figure 4.8 n'a point d'impact sur le nombre de paquets CBR rejetés avec FH-RSVP, malgré une augmentation du délai de l'Internet de 10 à 200 ms. Aucun paquet n'est perdu dans le cas FH-RSVP puisque, avant de débuter la relève, le MN reste au PAR jusqu'à ce que la connectivité soit perdue, nous sommes alors sûrs que lorsque nous recevons le message FBACK, il n'y a pas de paquets perdus envoyés au PAR et les paquets redirigés sont mis en tampon au NAR jusqu'à ce que la relève de niveau 2 se termine.

4.4.2 Le délai DMQ de mise à jour de la QdS

Les Figures 4.9, 4.10 et 4.11 donnent les courbes du délai de mise à jour de la QdS en fonction respectivement de la vitesse du MN, du débit de l'application et du délai de transmission de l'Internet *Id* pour les quatre scénarios FH-RSVP simulés et pour MRSVP. Les paquets CBR UDP émis à partir du CN vers le MN ont une taille de 200 octets. La durée des 5 scénarios simulés est de 1380 s à la Figure 4.9 et de 330 s aux Figures 4.10 et 4.11. Le débit de transmission des paquets est de 64kbps aux Figures 4.9 et 4.11 tandis qu'il varie selon le facteur *debit_pq* à la Figure 4.10.

Dans le cas du protocole MRSVP, un nœud qui se retrouve dans une cellule va faire une réservation dite active dans sa cellule courante et des réservations dites passives dans les cellules adjacentes à la cellule courante. Ainsi, si le délai DMQ est évalué par rapport aux réservations passives, il est évident que MRSVP sera plus rapide

que FH-RSVP puisque MRSVP réserve passivement des ressources avant même le déclenchement d'une relève.

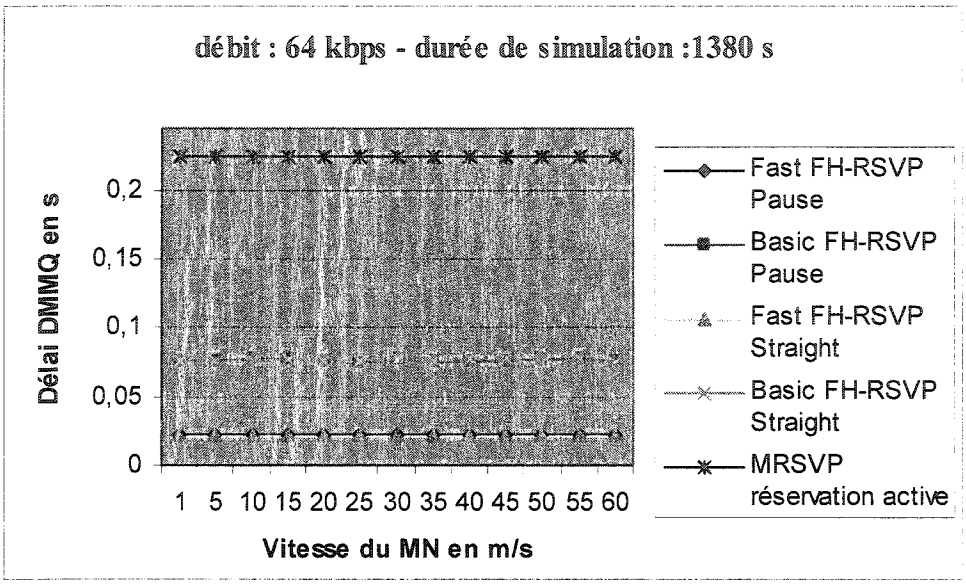


Figure 4.9 Délai moyen DMQ en fonction de la vitesse du MN

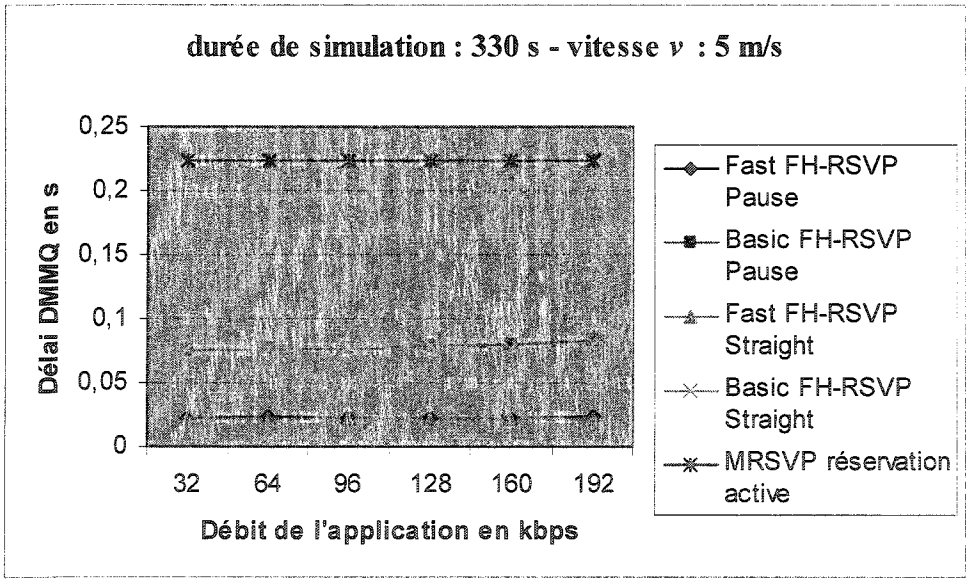


Figure 4.10 Délai moyen DMQ en fonction du débit de l'application

Par contre, lorsque le MN effectue une relève et qu'il se retrouve dans une nouvelle cellule à la fin de la relève de niveau deux, il faut activer les ressources passives dans la nouvelle cellule. Dans le cas MRSVP, le délai DMQ mesurera donc le délai encouru pour activer les ressources passives de la nouvelle cellule suivant une relève du MN. Nous utiliserons une borne inférieure du délai DMQ pour MRSVP, calculée à partir de l'équation (3.16). Pour un délai de transmission de l'Internet donné (i.e. 25 ms), nous obtenons une borne inférieure du délai DMQ MRSVP égale à 224 ms (Figures 4.9 et 4.10).

De manière générale, le délai moyen DMQ du protocole MRSVP pour activer les ressources passives dans la nouvelle cellule est toujours plus grand que celui du Basic FH-RSVP. Le délai moyen DMQ du mécanisme Basic FH-RSVP en moyenne de 70 à 80 ms (mode Pause et Straight) est toujours plus élevé que celui de Fast FH-RSVP (i.e. environs 21 ms). La vitesse du MN (Figure 4.9) et le débit de l'application (Figure 4.10) n'ont aucun impact sur le délai DMQ de MRSVP, de Basic FH-RSVP et de Fast FH-RSVP.

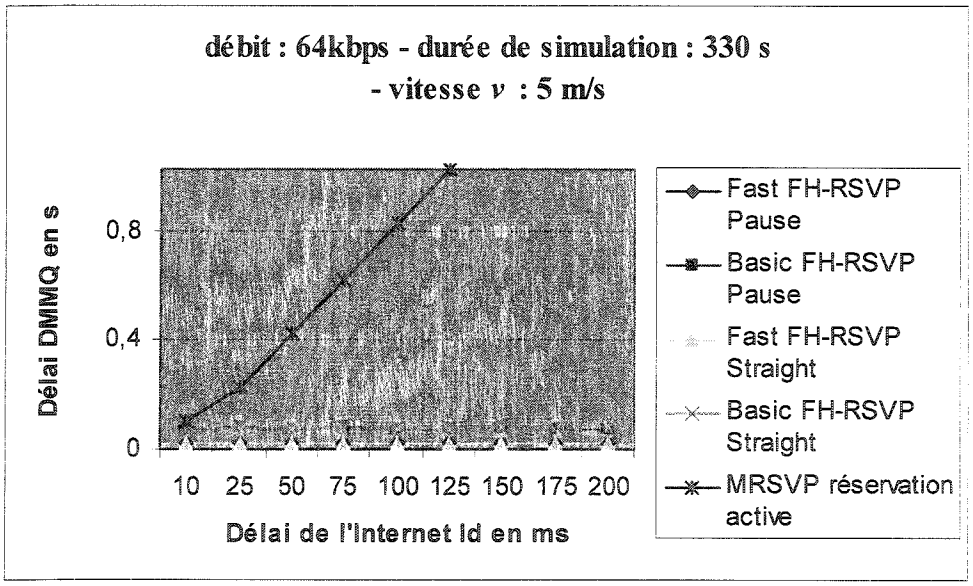


Figure 4.11 Délai moyen DMQ en fonction du délai de transmission de l'Internet

Dans le cas MRSVP, après que le temps TDH eut écoulé (temps que nous avons négligé), le MN se retrouve exclusivement dans la nouvelle cellule. Le nœud mobile MN envoie alors son M_Spec au CN, puis des messages de signalisation active PATH, active RESV et active ACK sont échangés entre le CN et le MN afin de réserver des ressources actives le long du chemin allant du CN au MN. Étant donné que la réinitialisation du nouveau chemin de QdS se fait de bout en bout entre le CN et le MN, le délai DMQ de MRSVP est grand. Plus le CN et le MN sont éloignés, ce qui correspond à une augmentation du délai de l'Internet *Id*, plus le délai DMQ de MRSVP sera grand. En effet, à la Figure 4.11, nous remarquons que le délai DMQ du protocole MRSVP croit proportionnellement avec le délai de l'Internet.

Dans Basic FH-RSVP, dès que le MN se retrouve exclusivement dans la nouvelle cellule, alors débute un échange de message de signalisation RESV et ACK entre le MN et le MAP. Les ressources sont uniquement modifiées sur la nouvelle portion de chemin allant du MN au MAP. Ainsi, nous pouvons constater à la Figure 4.13 que le délai de l'Internet n'a pas d'influence sur le délai DMQ de Basic FH-RSVP. Le délai DMQ de Basic FH-RSVP est alors beaucoup plus petit que celui de MRSVP parce que d'une part nous évitons une signalisation de bout en bout et d'autre part le mécanisme de réservation orienté émetteur est plus rapide que celui orienté récepteur utilisé dans MRSVP. Fast FH-RSVP est le mécanisme le plus rapide parmi les trois en terme de délai de mise à jour de la QdS (Figures 4.9, 4.10 et 4.11). En effet, sur réception de messages de niveau 2 (*L2 Trigger*) indiquant que le MN est en train de débuter une relève, le MN envoie un message *RtSolPr* vers le MAP. Sur réception du message *RtSolPr*, le MAP est en mesure de déclencher l'initialisation du nouveau chemin partant du MAP par l'échange de messages de signalisation RESV et ACK avec le MN. La rapidité de Fast FH-RSVP provient du fait que la réservation démarre dès que le MN franchit la zone de chevauchement, nous n'attendons pas qu'il se retrouve exclusivement dans la nouvelle cellule contrairement à MRSVP et Basic FH-RSVP. Pour les mêmes raisons que Basic FH-RSVP, le délai DMQ de Fast FH-RSVP ne dépend aucunement du délai de l'Internet (Figure 4.11).

4.4.3 Le débit

Les Figures 4.12 et 4.13 présentent les courbes du débit au nœud de réception MN au cours de la simulation pour le protocole MRSVP et FH-RSVP en mode Straight. Étant donné que les sous-mécanismes Basic et Fast FH-RSVP utilisent le même module de gestion de la mobilité et que nous n'avons pas surchargé le réseau, il est évident qu'ils auront le même débit. Ainsi, dans cette section l'utilisation de FH-RSVP fait référence aux deux sous-mécanismes. Dans les deux cas étudiés, le nœud mobile se déplace à une vitesse v de 5 m/s et les paquets CBR UDP de 200 octets sont transmis à un débit de 64 kbps. De façon générale, nous pouvons observer à la Figure 4.12 et à la Figure 4.13 que le MN réussit à maintenir un débit stable d'environ 64 kbps lorsqu'il se retrouve exclusivement à l'intérieur de la zone de couverture des routeurs d'accès suivants : AR1, AR2, AR3 et AR4.

Lorsque le protocole MRSVP est appliqué, le débit de transmission est toujours stable à 64 kbps parce que nous réservons à l'avance des ressources dans la nouvelle zone d'accès, excepté pendant le temps de latence. À la Figure 4.12, nous remarquons que ces trois moments instables sont caractérisés par une diminution du débit pendant les périodes de latence du *handoff* d'environ 2.15 s. Le délai de *handoff* est élevé parce que MRSVP utilise Mobile IPv4. Cela explique implicitement la perte de paquet élevée dans le cas MRSVP. D'autre part, lorsque FH-RSVP est appliqué, le débit de transmission est toujours stable à 64 kbps exclusivement dans chacune des zones d'accès parce que, comme MRSVP, nous réservons aussi à l'avance des ressources dans la future zone d'accès. FH-RSVP qui utilise les protocoles FMIPv6 et HMIPv6 permet de réduire le délai de handoff à environ 25 ms.

Les paquets CBR sont également transmis toutes les 25 ms (i.e. paquet de 200 octets transmis à 64 kbps). L'instabilité du débit de transmission sera donc moins marquée pendant le temps de latence puisqu'il est court.

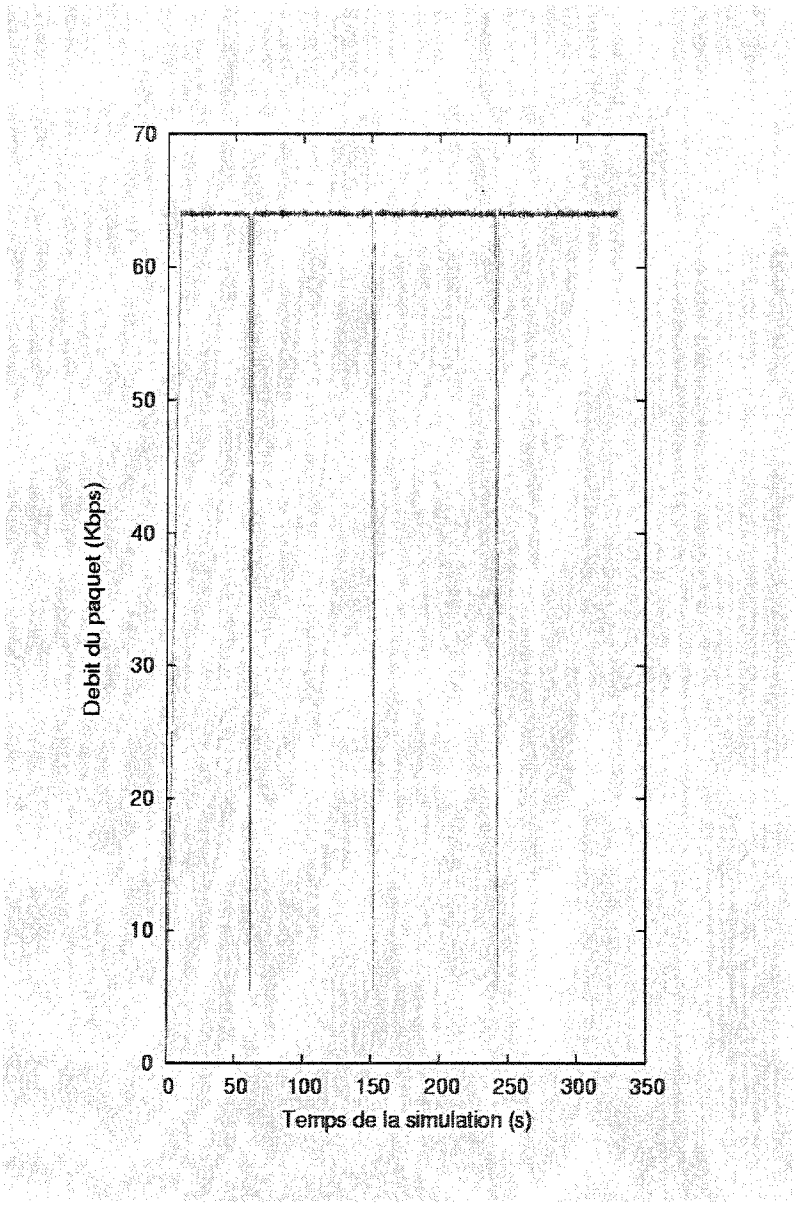


Figure 4.12 Débit au nœud MN – protocole MRSVP

De même, nous comprenons pourquoi la perte des paquets est nulle dans le cas FH-RSVP. Le mécanisme de QdS FH-RSVP diminue l'instabilité provoquée pendant la relève, contrairement à MRSVP.

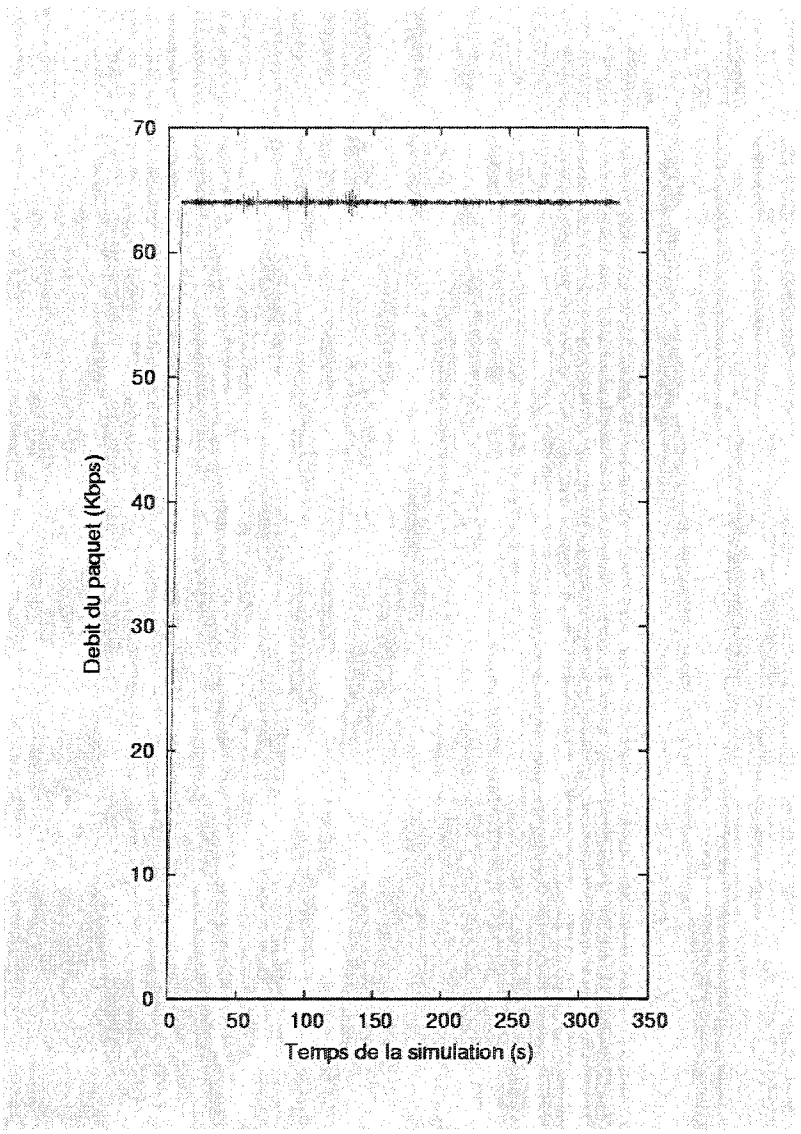


Figure 4.13 Débit au nœud MN – FH-RSVP

4.4.4 La latence de la relève

Les Figures 4.14, 4.16 et 4.18 présentent les courbes de la latence de la relève en fonction respectivement de la vitesse du MN, du débit de l'application et du délai de l'Internet *Id* pour les quatre scénarios FH-RSVP simulés (Fast FH-RSVP Pause, Basic FH-RSVP Pause, Fast FH-RSVP Straight, Basic FH-RSVP Straight) tandis que les Figures 4.15, 4.17 et 4.19 présentent le cas MRSVP. Les paquets CBR UDP émis à

partir du CN vers le MN ont une taille de 200 octets. La durée des 5 scénarios simulés est de 1380 s aux Figures 4.14 et 4.15 et de 330 s aux Figures 4.16, 4.17, 4.18 et 4.19. Le débit de transmission des paquets est de 64kbps aux Figures 4.14, 4.15, 4.18 et 4.19 tandis qu'il varie selon le facteur *debit_pq* aux Figures 4.16 et 4.17.

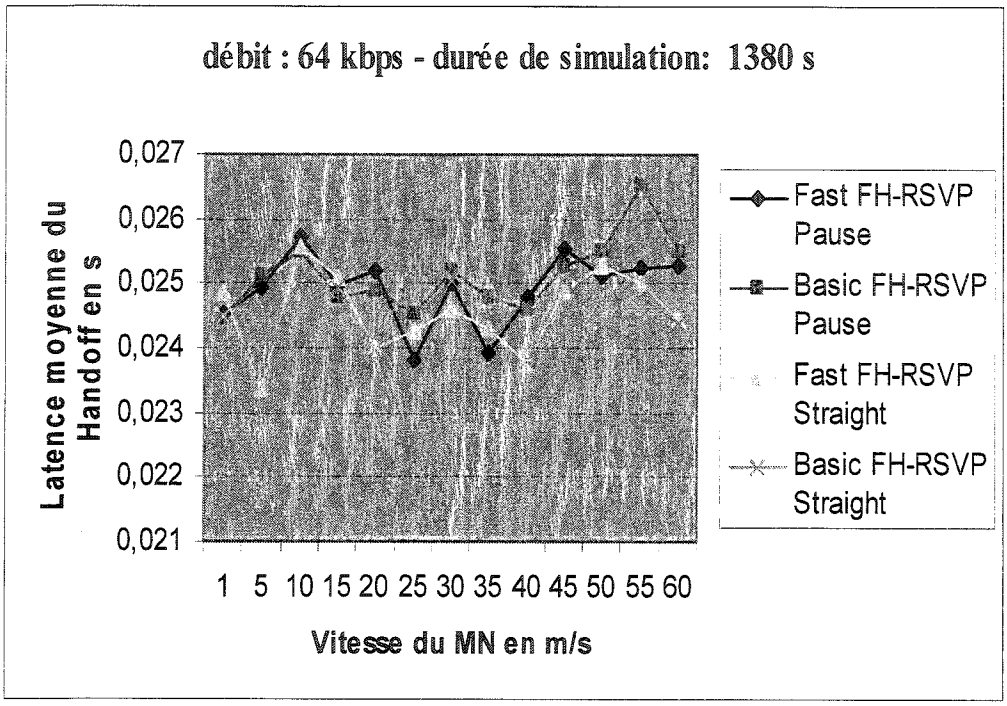


Figure 4.14 Latence de la relève en fonction de la vitesse du MN

De façon globale, la latence de la relève de MRSVP est toujours plus élevée (environ 2 à 2.5 s) que celle de FH-RSVP (environ 25 ms). Les courbes du délai de *handoff* à la Figure 4.14 de Fast FH-RSVP Pause, de Basic FH-RSVP Pause, de Fast FH-RSVP Straight et de Basic FH-RSVP Straight donnent respectivement en moyenne une latence de la relève égale à 24.93 ms, à 25.13 ms, à 24.58 ms et à 24.62 ms. Ces quatre courbes ne s'écartent pas trop de leurs latences moyennes respectives.

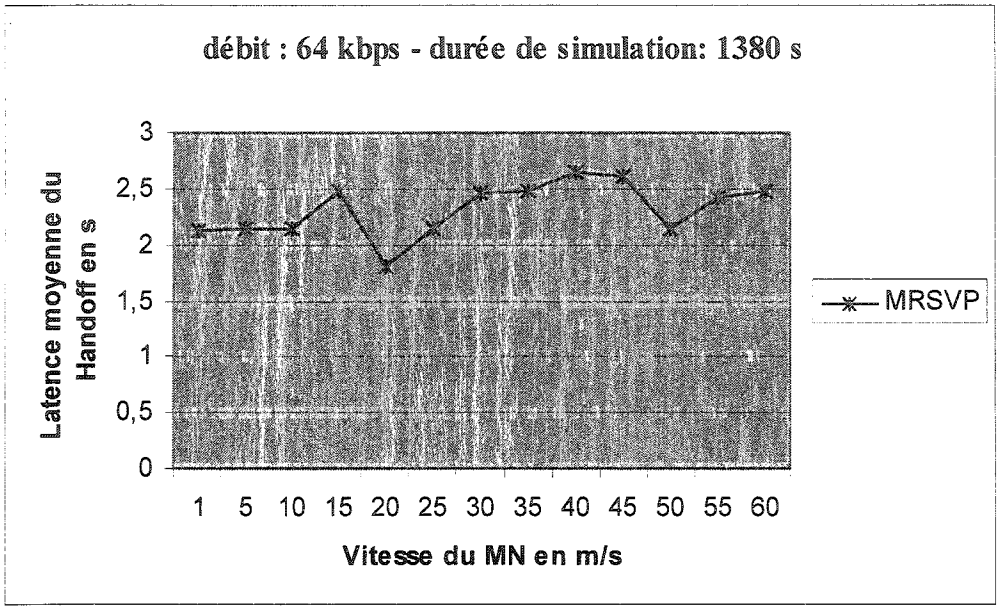


Figure 4.15 Latence de la relève et délai de l'Internet – MRSVP

La vitesse du MN n'a pas d'impact réel sur les courbes de latence de la relève observées.

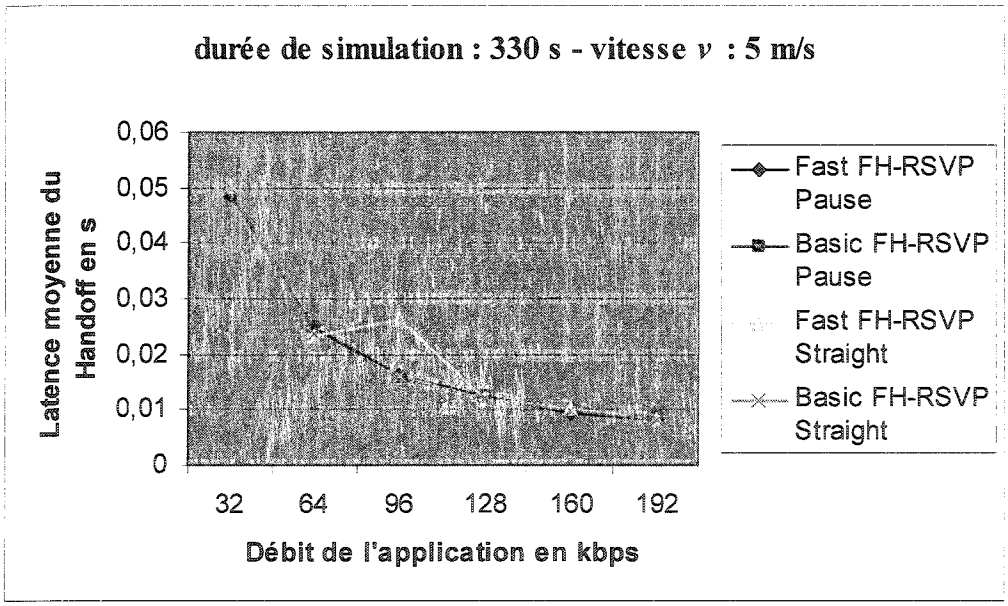


Figure 4.16 Latence de la relève et débit de l'application - FH-RSVP

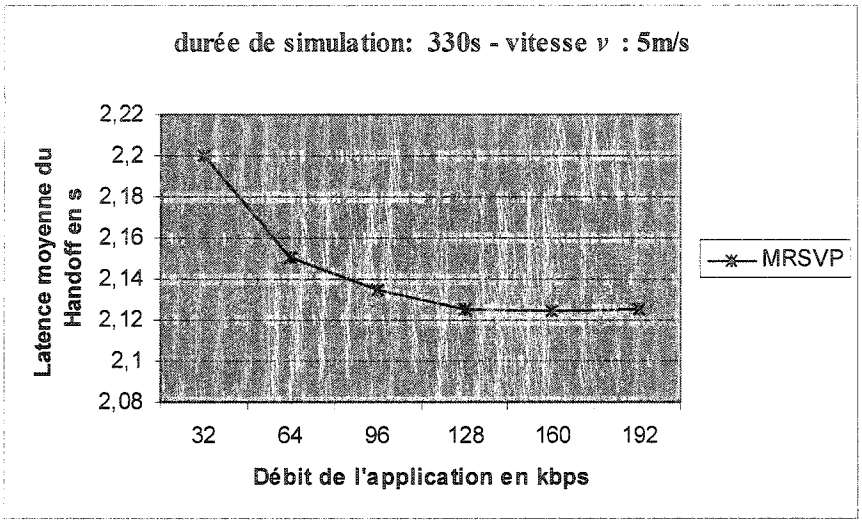


Figure 4.17 Latence de la relève et débit de l'application - MRSVP

Les Figures 4.16 et 4.17 montrent que la latence de la relève décroît avec une augmentation du débit de l'application. De par sa définition, la latence de la relève est le temps écoulé entre le dernier paquet reçu au PAR avec l'adresse *oldCoA* et le premier paquet reçu au NAR avec l'adresse *newCoA*. Une augmentation du débit entraîne automatiquement une diminution de l'intervalle auquel les paquets sont transmis, ce qui implicitement provoquera une baisse du temps de latence.

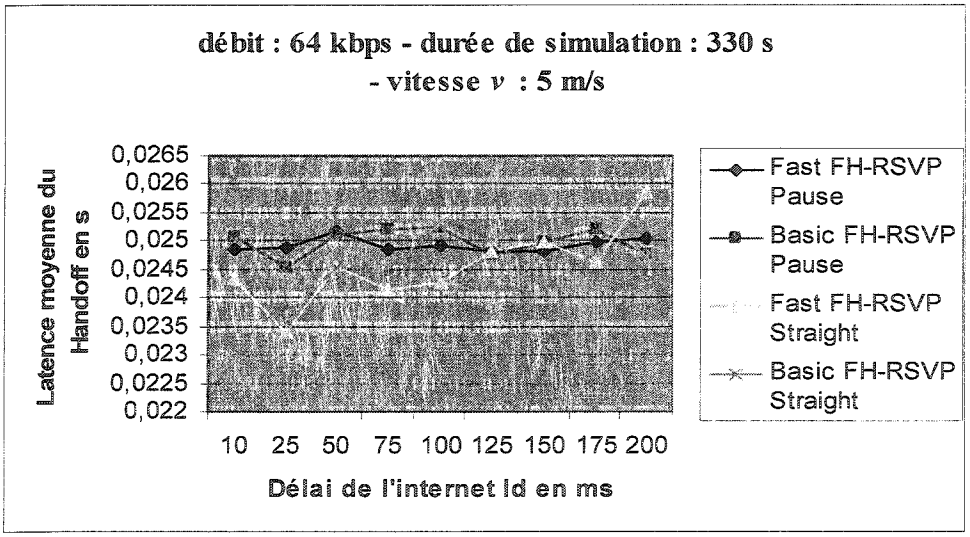


Figure 4.18 Latence de la relève et délai de l'Internet - FH-RSVP

À la Figure 4.18, les différentes valeurs de *Id* modélisent différentes distances du nœud N1 vers le HA et les CNs. Nous remarquons que la latence de la relève est en moyenne respectivement égale à 24.92 ms pour Fast FH-RSVP Pause, à 24.98 ms pour Basic FH-RSVP Pause, à 24,56 ms pour Fast FH-RSVP Straight et à 24.64 ms pour Basic FH-RSVP Straight. Pour les quatre scénarios étudiés, la latence de la relève varie très légèrement. FH-RSVP utilise une combinaison des protocoles FMIPv6 et HMIPv6 qui permet de réduire le temps qui s'écoule entre un changement de point d'attache du MN et la redirection du trafic vers sa nouvelle adresse *NLCoA*, par l'introduction d'une nouvelle entité de retransmission à l'intérieur du domaine local responsable de rediriger le trafic. En fait, c'est le MAP qui est en charge de la procédure de la relève rapide. La latence de la relève avoisine l'intervalle de transmission des paquets (autour de 25 ms).

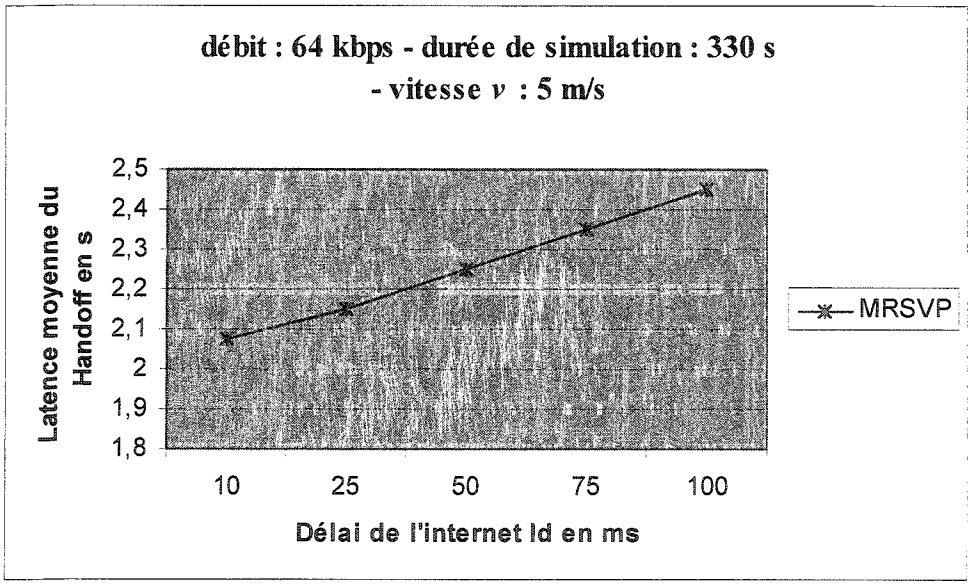


Figure 4.19 Latence de la relève et délai de l'Internet - MRSVP

La procédure classique de la relève rapide de redirection du PAR au NAR aurait été moins efficace en terme de latence de la relève puisque les paquets traverseraient deux fois les liens allant du MAP vers le PAR et l'ordre des paquets ne pourrait être garanti. Ainsi, le délai de la relève créé par le trafic redirigé ne dépend pas de la distance entre le MN et son HA et ses CNs hors du domaine local. Par contre, à la Figure 4.19,

MRSVP qui utilise Mobile IPv4 de base possède un délai de la relève qui est fonction du délai de transmission de l'Internet *Id.* Ainsi, nous observons que la latence augmente avec le délai *Id.*

4.4.5 Probabilité de blocage de réservation (P_b)

La Figure 4.20 montre les résultats de simulation pour la probabilité de blocage de réservation en fonction de la charge offerte pour le protocole MRSVP et le mécanisme FH-RSVP, avec β variant de 0.01 à 0.25 avec des valeurs intermédiaires (0.02, 0.03, 0.04, 0.05, 0.10, 0.15, 0.20). De façon générale, lorsque la charge offerte augmente, la probabilité de blocage de réservation augmente dans tous les cas analysés. Il est évident que plus la charge offerte est grande, moins les ressources sont disponibles.

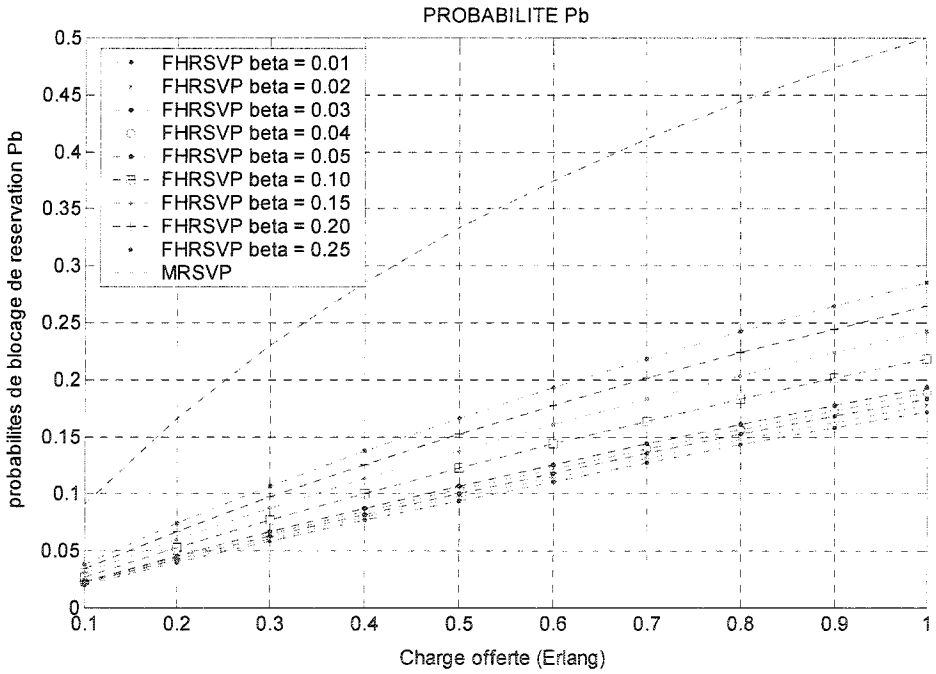


Figure 4.20 Probabilité de blocage de réservation

Cela entraîne implicitement une augmentation de la probabilité de blocage de la réservation. D'un autre coté, nous pouvons observer que la probabilité de blocage de réservation de MRSVP est plus élevée que celle de FH-RSVP avec β variant de 0.01 à

0.25. En effet, MRSVP réserve beaucoup plus de ressources dans les cellules adjacentes à la cellule courante que FH-RSVP.

FH-RSVP réserve uniquement des ressources pour les nœuds MNs présents dans les cellules adjacentes qui vont effectuer une relève vers la cellule courante (i.e. 4 βN avec β variant de 0.01 à 0.25) tandis que MRSVP réserve des ressources pour tous les MNs présents (au nombre de 4N) dans les cellules adjacentes.

Par exemple, avec une charge offerte de 0.3, la probabilité de blocage de réservation de MRSVP est de 23%, tandis qu'avec FH-RSVP, lorsque nous avons au total 25% (β=0.25) des MNs dans les cellules adjacentes qui migrent vers la cellule courante, la probabilité de blocage diminue de 12% (11%) par rapport à MRSVP. Pour β = 0.01, la probabilité de blocage de FH-RSVP est de 6%, soit une diminution de 17% par rapport à MRSVP.

4.4.6 Probabilité d'interruption forcée (P_f)

Les Figures 4.21 et 4.22 illustrent la probabilité d'interruption forcée dans le cas MRSVP et FH-RSVP, avec respectivement β égale à 0.01, 0.02, 0.03, 0.04 et 0.05, puis 0.05, 0.10, 0.15, 0.20 et 0.25 dans le cas d'une mobilité *indoor* (x=6). De même, les Figures 4.23 et 4.24 illustrent la probabilité P_f dans le cas MRSVP et FH-RSVP, avec respectivement β égale à 0.01, 0.02, 0.03, 0.04 et 0.05, puis 0.05, 0.10, 0.15, 0.20 et 0.25 dans le cas d'une mobilité *piétonne* (x=3). D'autre part, les Figures 4.25 et 4.26 illustrent la probabilité d'interruption forcée P_f dans le cas MRSVP et FH-RSVP pour les différentes valeurs de β, avec une mobilité *forte* (x=0.240).

Il est clair que, lorsque la charge offerte augmente, la probabilité P_f augmente aussi de façon générale. Nous observons que FH-RSVP est plus performant que MRSVP en terme de probabilité d'interruption forcée d'une réservation. Pour une mobilité donnée, la probabilité d'interruption forcée dans le cas MRSVP est totalement indépendante du facteur β. Ainsi, par exemple, pour la mobilité *indoor*, les courbes respectives de P_f pour MRSVP pour toutes les différentes valeurs de β se chevauchent

(Figure 4.21 et Figure 4.22). Étant donné une mobilité piétonne et une charge offerte de 0.5, la probabilité P_f de MRSVP est de 13.5%.

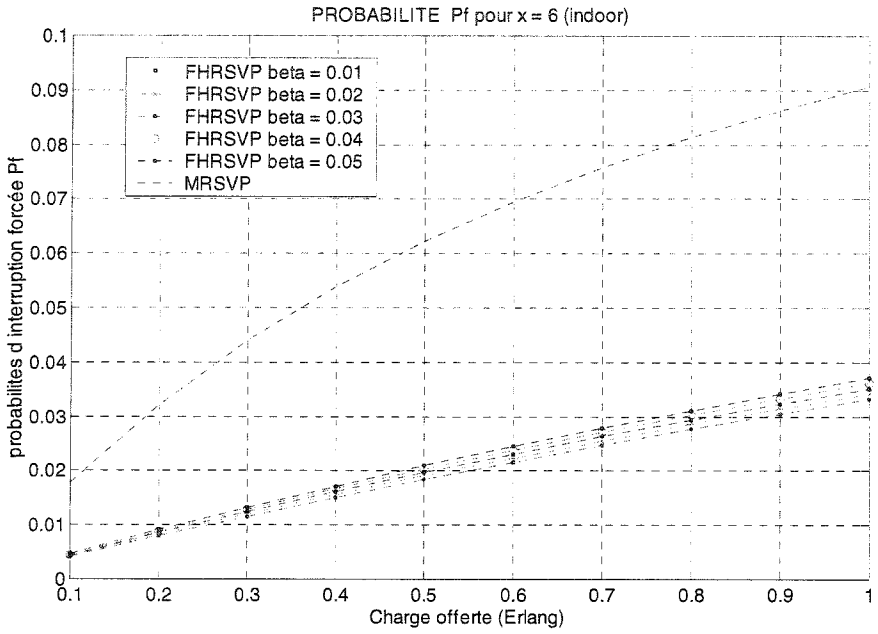


Figure 4.21 Probabilité P_f avec β = 0.01, 0.02, 0.03, 0.04, 0.05 –mobilité *indoor*

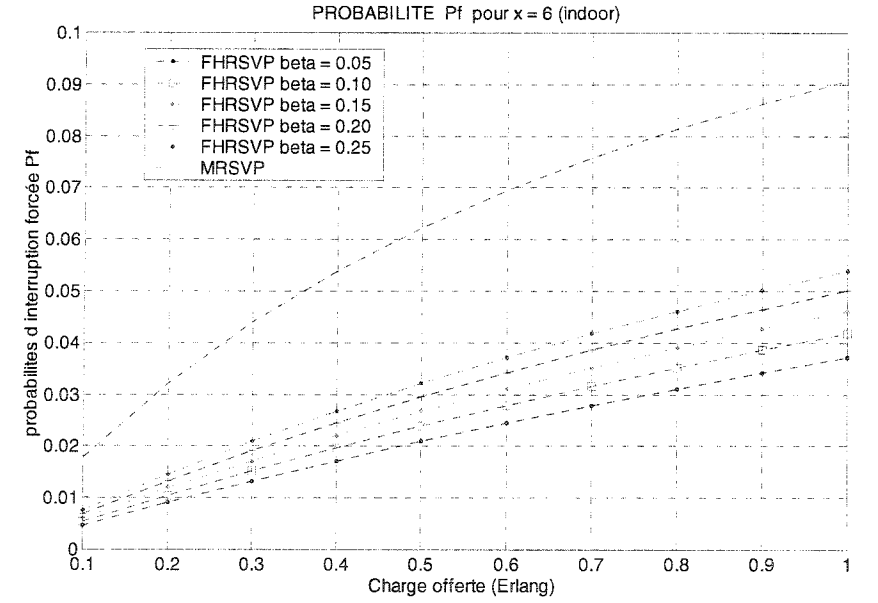


Figure 4.22 Probabilité P_f avec β = 0.05, 0.10, 0.15, 0.20, 0.25 –mobilité *indoor*

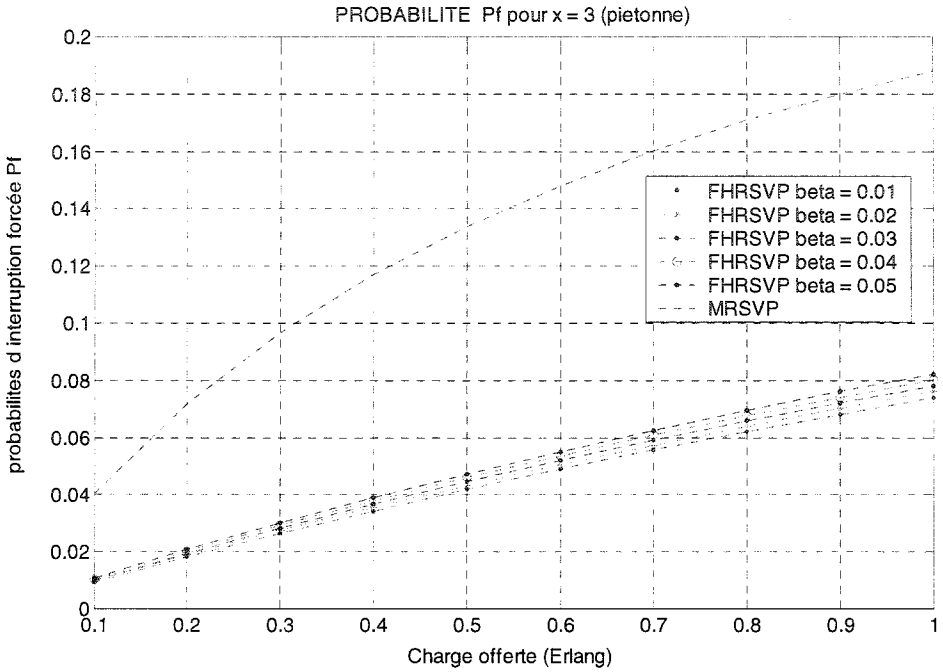


Figure 4.23 Probabilité P_f avec β = 0.01, 0.02, 0.03, 0.04, 0.05 –mobilité piétonne

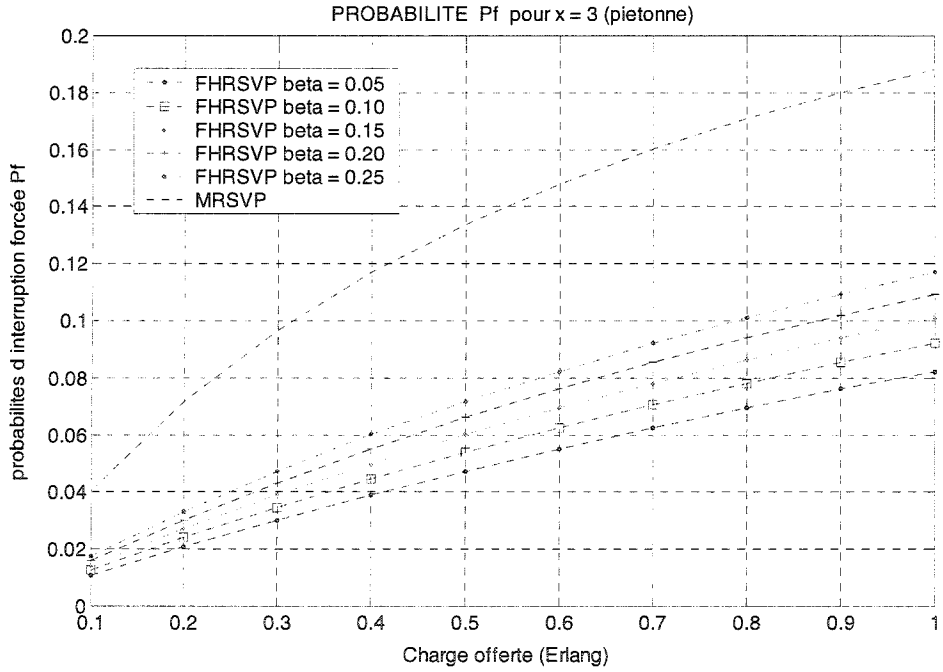


Figure 4.24 Probabilité P_f avec β = 0.05, 0.10, 0.15, 0.20, 0.25 –mobilité piétonne

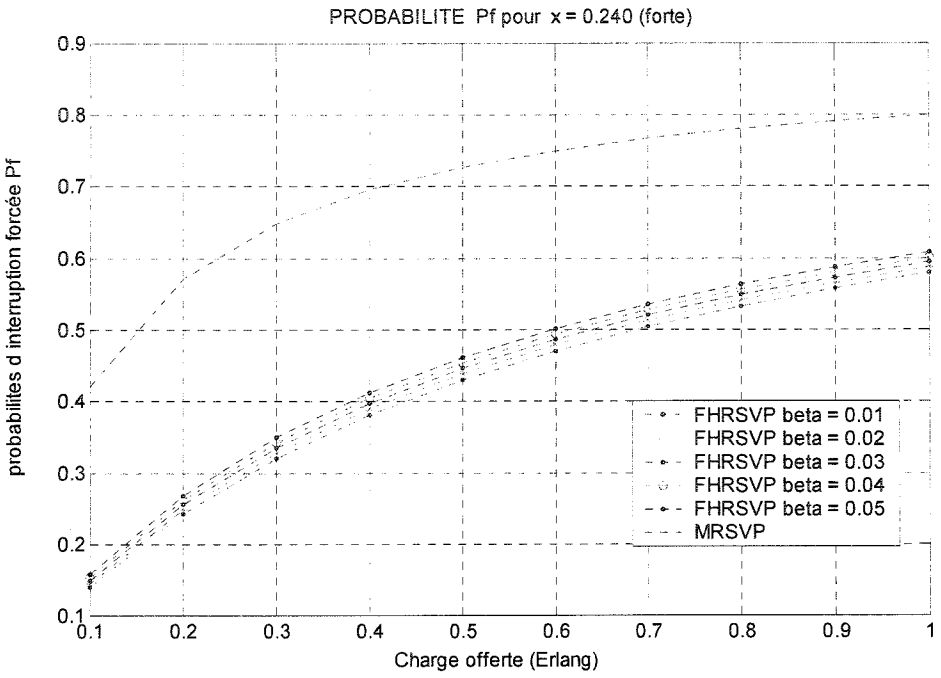


Figure 4.25 Probabilité P_f avec $\beta = 0.01, 0.02, 0.03, 0.04, 0.05$ –mobilité forte

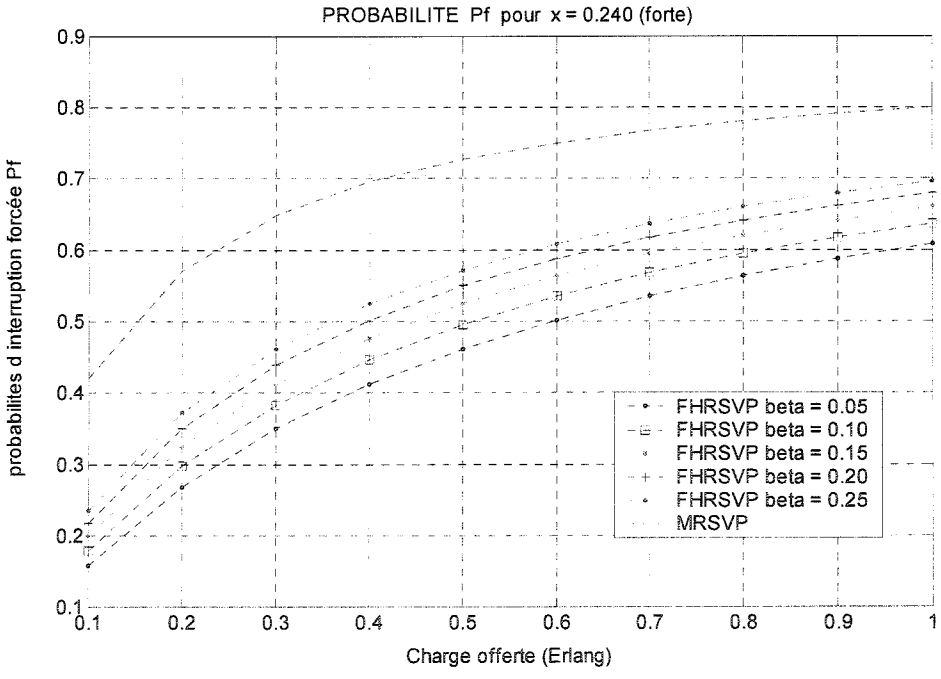


Figure 4.26 Probabilité P_f avec $\beta = 0.05, 0.10, 0.15, 0.20, 0.25$ - mobilité forte

FH-RSVP permet de diminuer la probabilité P_f de 6.3% avec β =0.25 (Figure 4.24), de 8% avec β =0.10 (Figure 4.24) et de 9.3% avec β =0.01 (Figure 4.23), par rapport à P_f de MRSVP. Le type de mobilité supportée par les MN a une influence sur la probabilité P_f. Plus la vélocité du nœud mobile augmente, plus le facteur x diminue, entraînant alors une augmentation de la probabilité d'interruption forcée dans le cas MRSVP et FH-RSVP. En effet, aux Figures 4.22, 4.24 et 4.26, pour une charge offerte de 0.3, la probabilité P_f de MRSVP est d'environ 4.5% pour la mobilité *indoor*, 9% pour la mobilité *piétonne* et 65% pour la mobilité *forte.*

4.4.7 Probabilité de compléter une session (P_c)

La probabilité de compléter une session est une combinaison des effets de la probabilité de blocage et d'interruption forcée de réservation. La Figure 4.27 montre la probabilité de compléter une session dans le meilleur des cas où nous avons supposé que la probabilité P_f est très faible par rapport à 1.

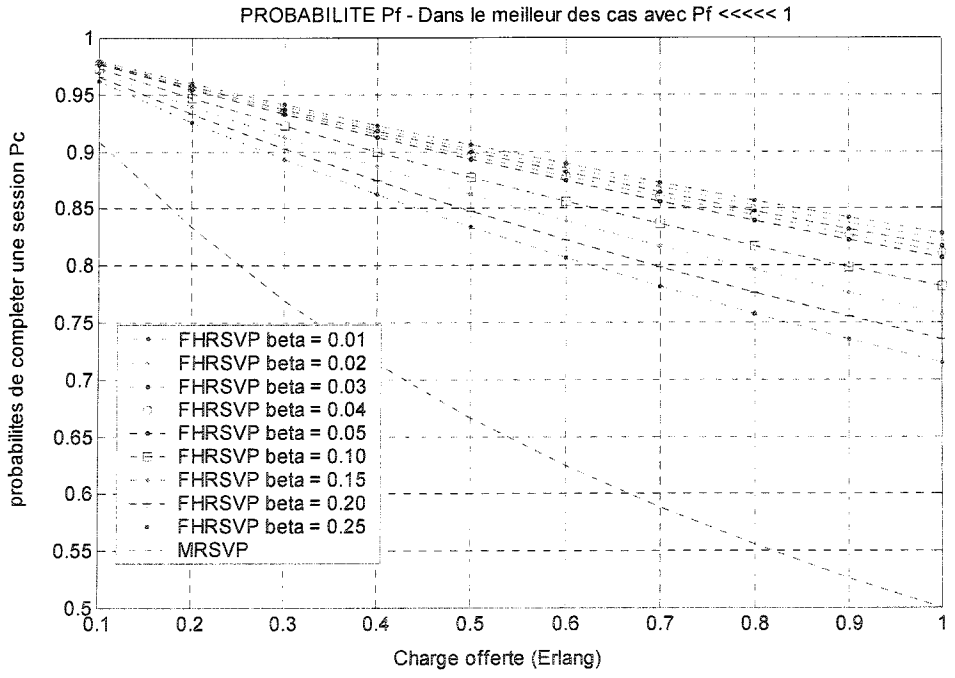


Figure 4.27 Probabilité P_c avec Pf <<<< 1

Lorsqu'on néglige la probabilité P_f, la probabilité de compléter une session P_c est automatiquement le complément de la probabilité de blocage de réservation présentée à la Figure 4.27.

De façon générale, lorsque la charge offerte augmente, la probabilité de compléter une session diminue dans tous les cas analysés. Il est évident que plus la charge offerte est grande, moins les ressources sont disponibles. Cela entraîne implicitement une diminution de la probabilité de compléter une session.

D'un autre coté, nous pouvons observer que la probabilité de compléter une session avec MRSVP est toujours plus petite que celle de FH-RSVP avec β variant de 0.01 à 0.25. Les Figures 4.28 et 4.29 illustrent la probabilité de compléter une session dans le cas MRSVP et FH-RSVP avec respectivement β égal à 0.01, 0.02, 0.03, 0.04 et 0.05, puis 0.05, 0.10, 0.15, 0.20 et 0.25 dans le cas d'une mobilité *indoor* ($x = 6$). Les Figures 4.30 et 4.31 illustrent la probabilité Pc de compléter une session dans le cas MRSVP et FH-RSVP pour différentes valeurs de β avec une mobilité *piétonne* ($x = 3$). Les Figures 4.32 et 4.33 illustrent la probabilité P_c dans le cas MRSVP et FH-RSVP pour différentes valeurs de β avec une mobilité *forte* ($x = 0.240$). Ainsi, nous couvrons, à l'aide du facteur x, l'ensemble des trois types de mobilité suivante : indoor, piétonne et forte.

Il est clair que lorsque la charge offerte augmente, la probabilité de compléter une session diminue de manière générale. Nous observons que FH-RSVP est plus performant que MRSVP en terme de probabilité de compléter une session. Pour une mobilité donnée, la probabilité de compléter une session dans le cas MRSVP est totalement indépendante du facteur β. Ainsi, par exemple, pour la mobilité *indoor*, les courbes respectives de P_c pour MRSVP pour les valeurs de β suivantes 0.01, 0.02, 0.03, 0.04, 0.05, 0.10, 0.15, 0.20, 0.25 se chevauchent (Figure 4.28 et Figure 4.29). Plus la mobilité diminue (i.e. la vélocité du nœud mobile diminue) plus le facteur x augmente, entraînant alors une augmentation de la probabilité de compléter une session dans le cas MRSVP et FH-RSVP.

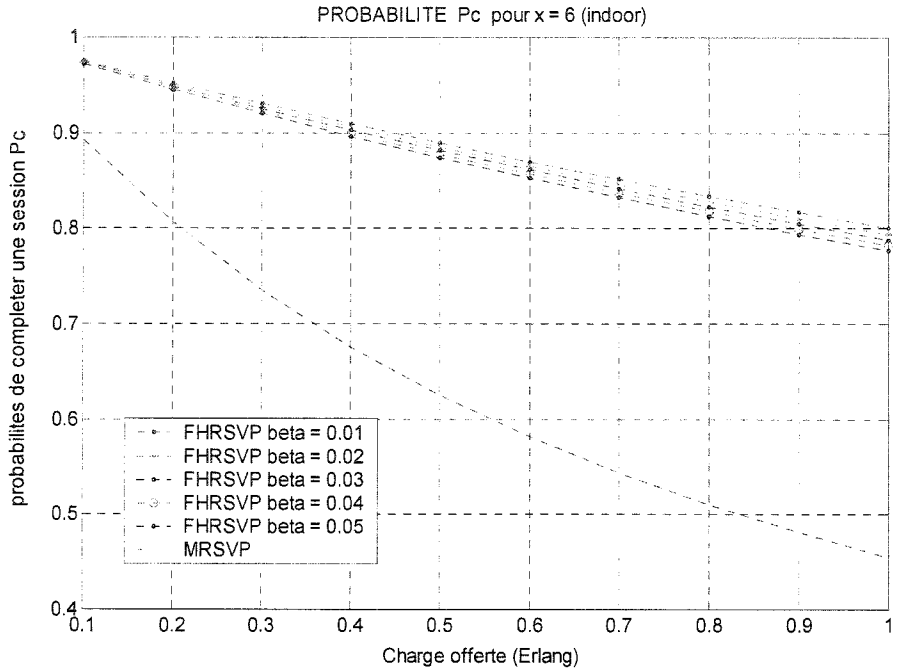


Figure 4.28 Probabilité P_c avec $\beta = 0.01, 0.02, 0.03, 0.04, 0.05$ –mobilité *indoor*

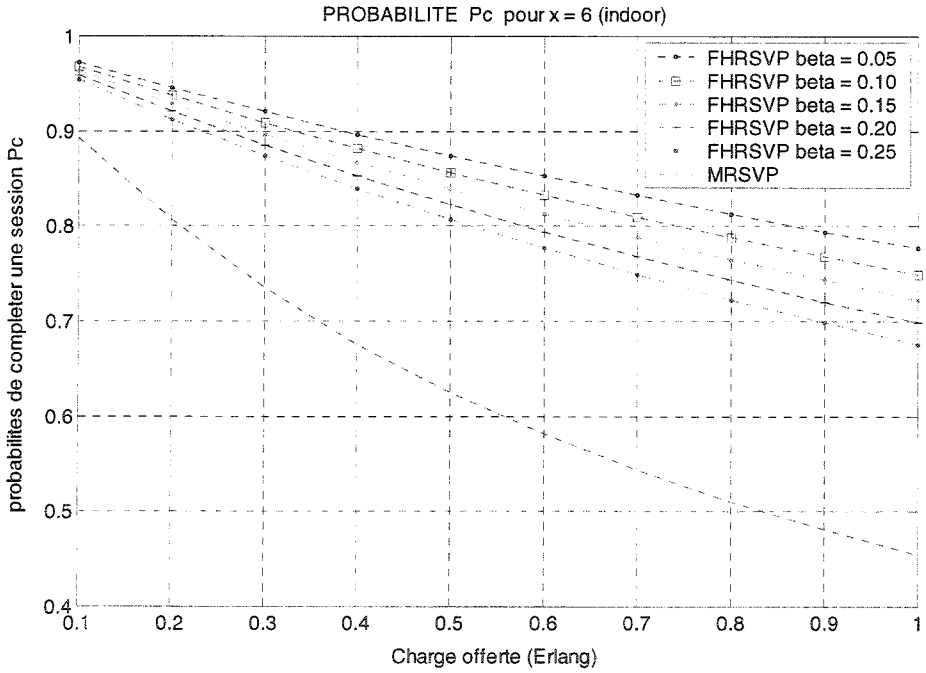


Figure 4.29 Probabilité P_c avec $\beta = 0.05, 0.10, 0.15, 0.20, 0.25$ –mobilité *indoor*

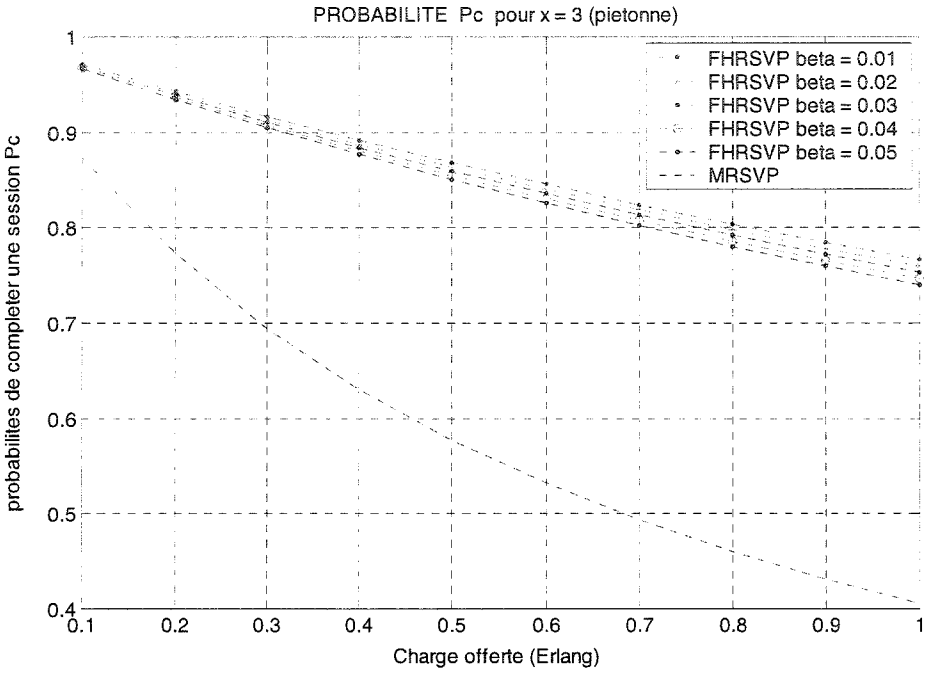


Figure 4.30 Probabilité P_c avec β = 0.01, 0.02, 0.03, 0.04, 0.05 –mobilité *piétonne*

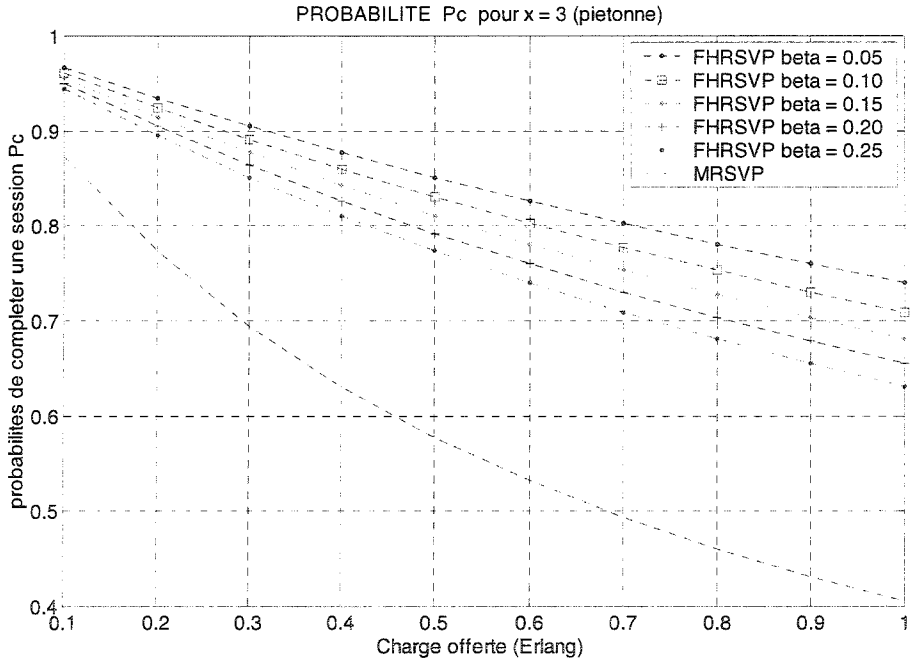


Figure 4.31 Probabilité P_c avec β = 0.05, 0.10, 0.15, 0.20, 0.25 –mobilité *piétonne*

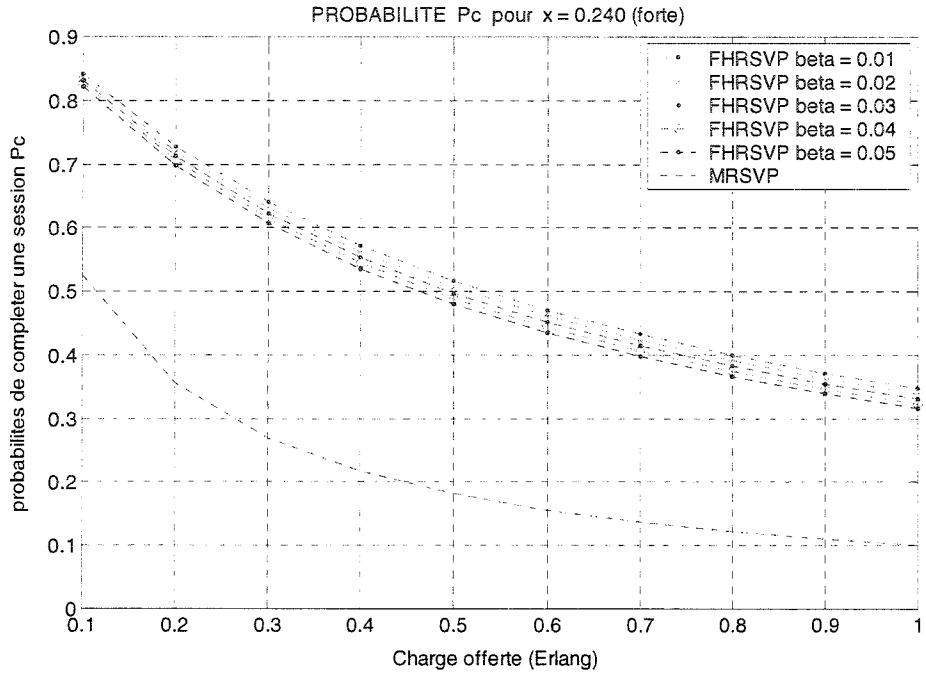


Figure 4.32 Probabilité P_c avec β = 0.01, 0.02, 0.03, 0.04, 0.05–mobilité *forte*

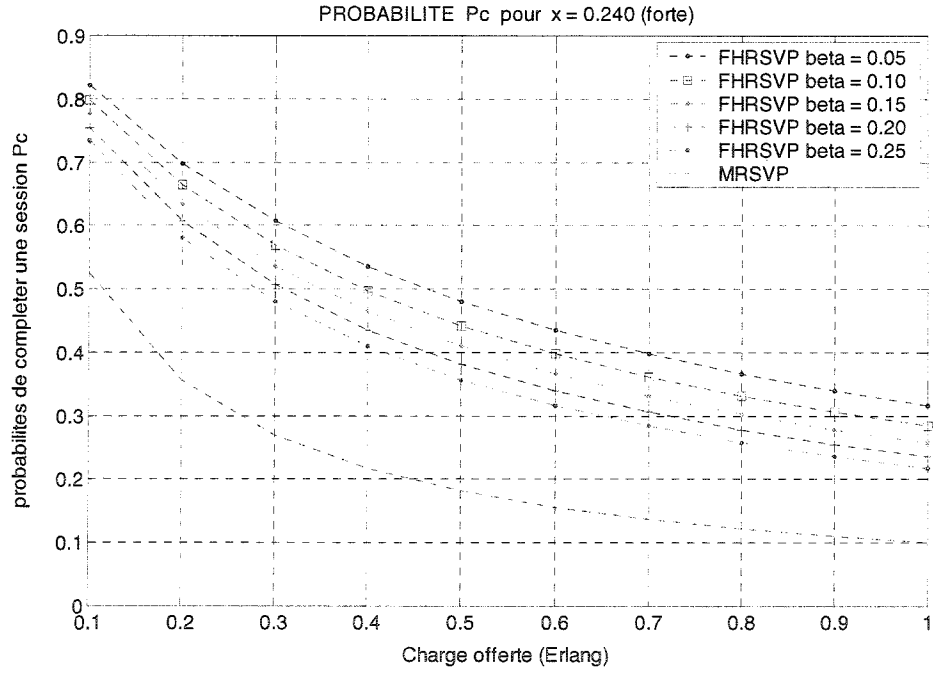


Figure 4.33 Probabilité P_c avec β = 0.05, 0.10, 0.15, 0.20, 0.25 –mobilité *forte*

Aux Figures 4.29, 4.31 et 4.33, pour une charge offerte de 0.3, la probabilité P_c de MRSVP est d'environ 27% pour la mobilité *forte*, 70% pour la mobilité *piétonne* et 74% pour la mobilité *indoor*. Étant donné une mobilité donnée dans le cas FH-RSVP, plus le facteur β augmente (i.e. plus le nombre de MN provenant des cellules adjacentes augmente), plus la probabilité P_c diminue. Par exemple pour une charge offerte de 0.3, dans le cas d'une mobilité *forte*, la probabilité P_c est de 64% pour $\beta = 0.01$ (Figure 4.32), de 58% pour $\beta = 0.10$ (Figure 4.33) et de 48% pour $\beta = 0.25$ dans le cas FH-RSVP.

CHAPITRE V
CONCLUSION

Dans ce mémoire, nous avons traité du problème de la qualité de service en terme de réservation de ressources d'un flot de données échangé entre le MN et son CN advenant une relève intra-site dans un environnement Hiérarchique Mobile IPv6. Nous avons considéré le cas d'applications temps réel. Nous avons proposé un mécanisme de QdS basé sur la réservation anticipée de ressources utilisant également les procédures de la relève rapide pour anticiper la relève intra-domaine MAP. Dans ce chapitre, nous allons faire une synthèse des travaux réalisés. Par la suite, nous présenterons les limites des méthodes proposées, puis nous donnerons un aperçu des travaux futurs.

5.1 Synthèse des travaux

Le problème de la gestion de la QdS dans un environnement *Mobile IPv6* revient à pouvoir combiner les protocoles de gestion de mobilité tels que *Mobile IPv6*, *Fast Mobile IPv6* ou *Hierarchical Mobile IPv6* avec un protocole de signalisation de QdS tels que *IntServ* avec *RSVP* ou *DiffServ*. Le but de notre travail était de concevoir une solution de QdS permettant de garantir la réservation de ressources pour des applications temps réel échangées entre le nœud mobile (MN) dont le medium radio est le WLAN et son nœud correspondant (CN), en tenant compte du processus de *handoff* intra-site du nœud MN. Il s'agissait également de développer un mécanisme de QdS rapide, efficace et peu glouton en terme de consommation de ressources.

Étant donné que 69 % de la mobilité est de la mobilité régionale ou dite micro-mobilité [17], nous avons choisi de bâtir notre mécanisme sur une architecture Hierarchical Mobile IPv6 et de consacrer nos efforts sur la relève intra-domaine MAP. Nous avons donc privilégié la méthode de réservation par anticipation en combinaison avec une variante du protocole RSVP, orienté émetteur, contrairement à RSVPv1 qui est orienté récepteur. En effet, le mode orienté émetteur permet un rétablissement rapide du chemin de QdS comparé à l'orienté récepteur. L'anticipation de la réservation utilise le

principe de la *relève rapide* pour réserver des ressources dès qu'une relève est détectée par FMIPv6. Nous avons présenté en détail le mode de fonctionnement de notre mécanisme FH-RSVP. Ce nouveau mécanisme définit un mode de réservation bidirectionnelle des ressources dans la zone d'accès du MN. Cela permet d'éviter un rétablissement de bout en bout le long du chemin allant du MN vers le CN, en réservant des ressources bidirectionnelles du MAP vers le NAR. Pour ce faire, le MAP qui est un agent *proxy* de QdS réserve des ressources sur le lien descendant au nom du CN et respectivement le PAR réserve des ressources sur le lien montant au nom du MN.

Nous avons implémenté deux versions de la méthode proposée, la différence fondamentale entre les deux provient du moment auquel est effectuée la mise à jour du nouveau chemin de QdS. En effet, dans la première méthode, Basic FH-RSVP, l'établissement du nouveau chemin de QdS se fait lorsque le MN se retrouve exclusivement dans la zone d'accès du routeur NAR sur réception d'un RA provenant uniquement du NAR. Cela indique le déplacement au niveau de la couche liaison. Pendant la période du *handoff*, les paquets reçus au routeur PAR qui seront redirigés vers le NAR sont traités en *best effort* jusqu'à ce que les ressources soient réservées. Le sous-mécanisme Basic FH-RSVP serait intéressant à utiliser lorsque le MN se retrouve dans une zone de chevauchement couvrant plus de deux zones d'accès (i.e. quatre zones d'accès par exemple). Puisque la mise à jour de la réservation bidirectionnelle sur le nouveau chemin intervient lorsque la relève au niveau radio est terminée, Basic FH-RSVP permet d'éviter de faire des réservations abusives dans les autres cellules adjacentes. Il permet une meilleure gestion des ressources disponibles. Basic FH-RSVP conviendrait à un environnement mobile dont le réseau d'accès du MN possède des ressources convenables mais pas énormes. De même, le temps de mise à jour de la QdS est satisfaisant pour des usagers exigeant une QdS de type gold ou premium.

Dans la seconde, Fast FH-RSVP, nous réalisons une réservation par anticipation. En effet, lorsque le MN reçoit un message de niveau 2 (L2-trigger) lui indiquant qu'il commence à franchir une zone de chevauchement entre le PAR et le NAR, le MN envoie un message *PrRtAdv* vers le MAP, contenant des informations sur

le futur routeur d'accès. Sur réception du *PrRtAdv*, le MAP qui est un agent de QdS réserve des ressources sur le lien descendant au nom du CN et, de même, le PAR réserve des ressources sur le lien montant au nom du MN. Ainsi, la différence majeure vient du fait que l'établissement du nouveau chemin de QdS s'amorce lorsque le MN est à l'intérieur de la zone de chevauchement dans le cas Fast FH-RSVP. Le sous-mécanisme Fast FH-RSVP serait intéressant à utiliser lorsque le MN se retrouve dans une zone de chevauchement couvrant au plus deux zones d'accès. Si nous avons plus de deux zones d'accès Fast FH-RSVP devient glouton car il gaspille les ressources disponibles. Fast FH-RSVP conviendrait à un environnement mobile dont le réseau d'accès du MN possède d'énormes ressources disponibles sinon cela nécessiterait l'ajout d'un mécanisme de gestion des ressources. De même, le temps de mise à jour de la QdS d'environs 21ms permet une garantie de la qualité de services pour les applications critiques temps réel.

À l'aide du simulateur NS-2, nous avons étudié les effets des variations de trois facteurs sur le délai de mise à jour de la QdS (DMQ), sur le débit de l'application au nœud MN, sur la latence de la *relève* et sur la perte de paquet soit : la vitesse du nœud mobile MN, le débit de l'application et le délai de transmission de l'Internet *Id.* D'autre part, MATLAB nous a permis de faire l'étude de l'impact des facteurs sur les probabilités de blocage de réservation, d'interruption forcée de réservation, de compléter une session soit : la charge totale offerte, le pourcentage total de MNs provenant des cellules adjacentes qui font un *handoff* vers la cellule courante et le terme x (ou $\mu L/V$) qui dépend de la vitesse relative du nœud MN.

Pour évaluer la performance de Fast FH-RSVP et de Basic FH-RSVP, nous avons comparé nos résultats à ceux obtenus avec le protocole MRSVP. Dans tous les cas, les résultats obtenus étaient meilleurs que ceux de MRSVP sur NS-2 comme sur MATLAB.

5.2 Limitations des travaux

Dans l'ensemble, nous avons obtenu de bons résultats. Cependant, notre travail comporte certaines limites. En effet, lors des simulations sur NS-2, nous avons considéré qu'un unique nœud mobile se déplace et communique avec un nœud CN. En faisant cela, les méthodes proposées ne peuvent être bien évaluées sur NS-2 parce que nous évitons de surcharger le réseau. Une telle surcharge aurait sans doute eu un impact sur le débit de réception de l'application au nœud MN observé. Par contre, nous tenons compte de cet aspect du problème dans l'étude faite sur MATLAB avec l'évaluation des probabilités P_b, P_f et P_c.

Nous avons choisi un déplacement déterministe du nœud mobile pour vérifier le bon fonctionnement de notre mécanisme FH-RSVP suivant plusieurs relèves. Notons cependant que les mouvements aléatoires, donc non prévisibles peuvent avoir un impact très négatif sur le nombre de paquets rejetés (perdus) dû aux mouvements de va et vient autour de la zone de chevauchement.

5.3 Travaux futurs

Pour résoudre le problème de la QdS, nous n'avons considéré que la relève intra-domaine MAP. Un point intéressant serait d'étendre ou d'améliorer FH-RSVP afin qu'il puisse également supporter la relève inter-domaine MAP bien qu'elle survienne très rarement. De cette manière, FH-RSVP supporterait tous les cas de relèves possibles dans un environnement HMIPv6. Il serait également intéressant d'étudier d'une part l'effet d'autres nœuds mobiles en mouvement sur le nœud MN observé et d'autre part l'impact du nombre de nœuds correspondants sur le nœud MN observé. Il existe également d'autres facteurs qui pourraient influencer les performances de FH-RSVP tel que la taille de la zone de chevauchement, le taux de *handoff*, le temps pour extraire les réservations sur un chemin, le type de mouvement du MN (exemple: cas aléatoire).

Finalement, il serait intéressant d'appliquer une politique de gestion des ressources réservées (i.e. CAC) afin d'améliorer les performances de FH-RSVP en terme

de probabilités de blocage de réservation, d'interruption forcée de réservation et de compléter une session.

BIBLIOGRAPHIE

[1] D. Johnson, C. Perkins et J. Arkko. Mobility Support in IPv6. RFC 3775, IETF, Juin 2004.

[2] IETF Integrated Services Working Group. See http://www.ietf.org/tml-charters/intserv-charter.html.

[3] IETF Differentiated Services Working Group. See http://www.ietf.org/html-charters/diffserv-charter.html.

[4] H. Chaskar. Requirements of a Quality of Service (QoS) Solution for Mobile IP. RFC 3583, IETF, Septembre 2003.

[5] R. Koodli, G. Dommety, A. Yegin, C. Perkins, G. Tsirtsis, K. El-Malki et M. Khalil. Fast Handovers for Mobile IPv6. Internet Draft, draft-ietf-mipshop-fast-mipv6-02.txt, Juillet 2004.

[6] H. Soliman, C. Castelluccia, K. El-Malki et L. Bellier. Hierarchical MIPv6 mobility Management (HMIPv6). Internet Draft, draft-ietf-mipshop-hmipv6-02.txt, Décembre 2004.

[7] S. Yasukawa, J. Nishikido et K. Hisashi. Scalable Mobility and QoS Support Mechanism for IPv6-based Real-time Wireless Internet Traffic. in: *Proceedings of GLOBECOM'01, IEEE*, Vol. 6, Novembre 2001, San Antonio, TX USA, pp. 3459-3462.

[8] K. Nichols, S. Blake, F. Baker et D. Black. Definition of Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474, IETF, Décembre 1998.

[9] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang et W. Weiss. An architecture for Differentiated Services. RFC 2475, IETF, Décembre 1998.

[10] A. Terzis, M. Srivastava et L. Zhang. A simple QoS signalling protocol for mobile hosts in the integrated services Internet. in: *Proceedings of INFOCOM'99, IEEE*, Vol. 3 Mars 1999, New York, NY USA, pp. 1011-1018.

[11] X. Fu, H. Karl G. Schaefer, C. Fan, C. Kappler et M. Schramm. QoS-conditionalized Binding Update in Mobile IPv6. Internet Draft, draft-tkn-mobileip-qosbinding-mipv6-00.txt, 13 Juillet 2001.

[12] W. Chen et L. Huang. RSVP mobility support: a signalling protocol for integrated services internet with mobile hosts. in: *Proceedings of INFOCOM'00, IEEE*, Vol. 3, 26-30, Mars 2000, Tel-Aviv, Israel, pp.1283-1292.

[13] A. Talukdar, B. Badrinath et A. Acharya. MRSVP: a resource reservation protocol for an integrated services network with mobile hosts. *The Journal of Wireless Networks*, Vol.7, No.1, Janvier 2001, pp. 5-19.

[14] R. Braden et L. Zhang. Resource ReSerVation Protocol (RSVP) – Version 1 Message Processing Rules. RFC 2209, IETF, Septembre 1997.

[15] L. Zhang, S. Deering, D. Estrin, S. Shenker et D. Zappala. RSVP: a new resource ReSerVation Protocol. *IEEE Network*, Vol.7, No.5, Septembre 1993, pp. 8-18.

[16] C. Perkins, Ed. IP Mobility Support for IPv4. RFC 3344, IETF, Août 2002.

[17] C. Castelluccia. HMIPv6: A Hierarchical Mobile IPv6 Proposal. ACM SIGMOBILE Computing and Communications Review , Vol. 4, No. 1, Janvier 2002, pp. 48-59.

[18] C. Tseng, G. Lee et R. Liu. HMRSVP: A Hierarchical Mobile RSVP protocol. *Wireless Network*, Vol. 9, 2003, pp. 95-102.

[19] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. SIP: Session Initiation Protocol. RFC 3261, IETF, Juin 2002.

[20] W. Fenner. Internet Group Management Protocol, Version 2. RFC2236, IETF, Novembre 1997.

[21] C Perkins et D. Johnson. Route optimisation in Mobile IP. Internet Draft, draft-ietf-mobileip-optim-12.txt (work in progress).

[22] C. Shen, W. Seah, A. Lo, H. Zheng et M. Greis. An interoperation Framework for Using RSVP in Mobile IPv6 Networks. Internet Draft, Juillet 2004.

[23] H. Chaskar et R. Koodli. A Framework for QoS Support in Mobile IPv6. Internet Draft, draft-chaskar-mobileip-qos-01.txt, Mars 2001.

[24] The UCB/LBNL/VINT Network Simulator – NS-2 (version 2). http://www.isi.edu/nsnam/ns.

[25] J. Widmer. Wireless Extension to the NS Network Simulator. Voir http://www.icsi.berkeley.edu/~widmer/mnav/ns-extension/.

[26] C. Bettestetter, H. Hartenstein, and X. Perez-Costa. Stochastic Properties of the Random Waypoint Mobility Model. in: *ACM Kluwer Wireless Networks, special issue on Modeling & Analysis of Mobile Networks* (*WINET*), Mars 2003, pp 7-14.

[27] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specicifications. IEEE Standard 802.11, June 1999.

[28] C. Perkins. IP encapsulation within IP. RFC 2003, October 1996.

[29] R. Hsieh, A. Seneviratne et K. El-Malki. Performance analysis on Hierarchical Mobile IPv6 with Fast-Handoff over End-to-End TCP. in: *Proceedings of GLOBECOM2002,* Vol. 21, No.1, Novembre 2002, Taipei, Taiwan, pp. 2500-2504.

[30] X. Perez-Costa, M. Torrent-Moreno et H. Hartenstein. A Simulation Study on the Performance of Hierarchical Mobile IPv6. in: *Proceedings of International Teletraffic Congress (ITC)*, 2003.

[31] H. Soliman, H. Jung, S. Koh, J. Lee, K. El-Malki, B. Hartwell, Fast Handover for Hierarchical MIPv6 (F-HMIPv6), Internet Draft, draft-jung-mobileip-fastho-hmipv6-04.txt, June 2004.

[32] X. Perez-Costa, M. Torrent-Moreno et H. Hartenstein. A Performance Comparison of Mobile IPv6, Fast Handovers for Mobile IPv6 and their combination. *Mobile Computing and communication review*, Vol. 7, No. 4, 2003.

[33] M. Greis. Module RSVP/ns: ns-2 extension to study RSVPv1 protocol. *Contributed Modules*, http://www.isi.edu/nsnam/ns/ns-contributed.html.

[34] R. Hsieh. fhmip ns-extension: source code for ns-extension on HMIPv6 with Fast-Handover. http://mobqos.ee.unsw.edu.au/~robert/nstut.php.

ANNEXE

Nous débuterons par une démonstration de la probabilité de *handoff* P_h. Puis nous présenterons les détails de la structure interne de l'implémentation de FH-RSVP sur NS-2. Nous terminerons cette annexe par une présentation de résultats complémentaires, sur le délai de bout en bout, ainsi qu'une analyse de ceux-ci.

a.1 Démonstration de la probabilité P_h

Nous posons les hypothèses suivantes afin de faire notre analyse :

- toutes les cellules sont identiques de longueur L, et le MN se déplace le long de la longueur L des cellules ;
- les mobiles se déplacent selon une vélocité V ;
- le temps de maintenance d'un appel suit une loi exponentielle avec pour moyenne $1/\mu$;
- la distance que les nouveaux appels ont à traverser avant leur première tentative de relève est uniformément distribuée entre 0 et L. Cette hypothèse se justifie parce que les MNs peuvent démarrer un appel à partir de n'importe quelle position dans une cellule. Ainsi, une relève devra être faite après que la distance restante dans la cellule est traversée.

Nous désignons par *cellule source,* la cellule d'origine d'un appel et par *cellule transit*, la cellule vers laquelle un appel se retrouve. Un mobile dans sa cellule source doit traverser une distance qui est uniformément distribuée entre 0 et L avant sa première relève. Un MN qui pénètre dans sa cellule transit, doit traverser une distance fixe L avant sa prochaine relève, à moins qu'il finisse son service avant sa future relève. Soit Y la variable aléatoire représentant la distance qu'un MN doit faire dans sa cellule source avant de faire une relève.

Ainsi, la probabilité P_h qu'un MN dans sa cellule source effectue une relève est :

$$P_h = \int_0^L P[T_m \geq \frac{y}{V}] f_y(y)dy,$$

$$f_y(y) = \frac{1}{L} \quad \text{si } 0 \leq y \leq L, \text{ sinon } 0$$

$$P_h = \frac{1 - e^{-\mu L/V}}{\mu L/V}$$

De même, un MN dans sa *cellule transit* effectue une autre relève selon la probabilité P_h suivante :

$$P_h = e^{-\mu L/V}$$

a.2 Structure interne de l'implémentation RSVPv2/NS

Les algorithmes ont été implémentés en C++ et OTcl (Figure a.1) avec le simulateur NS-2. Nous avons privilégié une structure de programmation orientée objet à cause de l'interaction entre les éléments à programmer. De plus, l'utilisation d'objets facilite la compréhension du code.

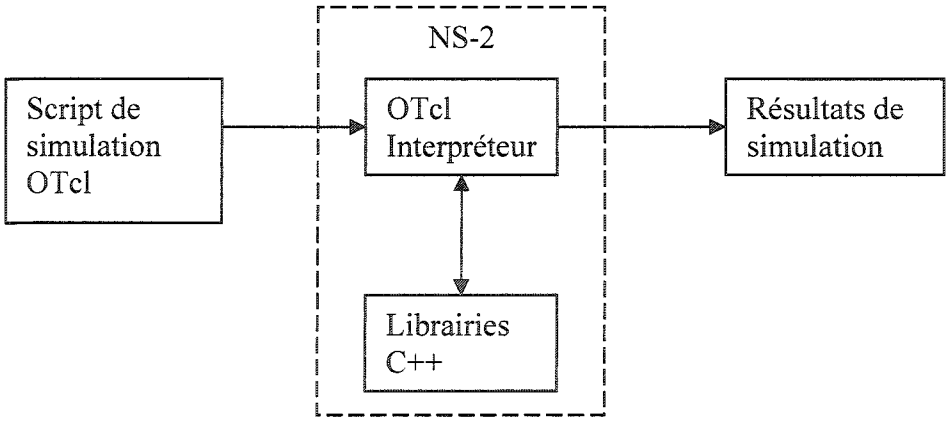


Figure a.1 Implémentation sur NS-2

L'un des objectifs du design de RSVPv2/NS était de le rendre le plus indépendant possible de l'implémentation propre de NS-2 et de ne pas modifier des fichiers appartenant à NS-2 à moins que cela ne soit strictement indispensable, pour permettre une compatibilité avec les versions futures de NS-2.

A- La classe RSVPv2objet

La classe *RSVPv2object* est la classe de base pour tous les objets RSVPv2. Ses attributs principaux sont :

- *objheader* : l'entête commune pour tous les objets RSVPv2 qui est composée des champs suivants :
  - *lenght* : la taille simulée de l'objet ;
  - *conlenght* : la taille réelle des contenus de l'objet ;
  - *classnum* : identificateur entier qui permet de distinguer les objets RSVPv2 [14] et [15] ;
  - *ctype* : correspond au C-Type défini en [14] et [15].
- *contents* : un pointeur vers la mémoire qui contient les contenus de l'objet RSVPv2.

Les valeurs du champ "*lenght*" peuvent varier selon les objets qui ont été créés pour des simulations IPv4 ou IPv6, tandis que le champ *conlenght* est toujours le même. Le Tableau a.1 montre les différents objets RSVPv2 implémentés dans RSVPv2/NS.

Tableau a.1 Les objets RSVPv2 dans RSVPv2/ns

Objet	Class-Num
SESSION2	1
RSVP_HOP2	3
TIME_VALUES2	5
ERROR_SPEC2	6
STYLE2	8
FLOWSPEC2	9
FILTER_SPEC2	10
SENDER_TEMPLATE2	11
SENDER_TSPEC2	12
RESV_CONFIRM2	15
RECEIVER_TEMPLATE2	19
MAP_TEMPLATE	21

Tous ces objets ont été implémentés afin de représenter les longueurs des objets pour IPv4 et IPv6.

B- La classe RSVPv2Message

La classe *RSVPv2message* est la classe de base pour tous les messages RSVPv2. Ses attributs principaux sont :

- *common_header* : l'entête commune pour tous les messages RSVPv2 qui est composée des champs suivants :
  - *type* : le type de message RSVPv2 ;
  - *lenght* : la taille simulée de l'objet ;
  - *conlenght* : la taille réelle des contenus de l'objet ;
  - *send_TTL* : TTL_IP à partir duquel le message a été transmis.
- *contents* : un pointeur vers la mémoire qui contient les contenus du message RSVPv2.

Ainsi, la mémoire *contents* d'un *RSVPv2message* est constituée à partir des mémoires *contents* des *RSVPv2objects* qu'il contient. Les valeurs du champ *lenght* peuvent varier selon les messages qui ont été créés pour des simulations IPv4 ou IPv6, tandis que le champ *conlenght* est toujours le même. La taille du message est calculée comme la somme de la taille des objets augmentée de la taille de l'entête IP appropriée (IPv6 ou IPv4)

Les quatre types de message suivants ont été implémentés dans RSVPv2 /NS :

- *Resvv2* : diffère légèrement du message *Resv* de RSVP car il est composé de certains objets de *Path* et de *Resv* de RSVPv1 ;
- *ResvTearv2* : est identique au *ResvTear* de RSVPv1 ;
- *ResvErrv2* : contient les mêmes objets que *ResvErr* de RSVPv1, par contre le message *ResvErrv2* est émis à partir du nœud où l'erreur s'est produite vers le nœud émetteur ;

- *Ackv2* : contient les mêmes objets que le *ResvConf* de RSVPv1, mais le message *Ackv2* est émis du nœud récepteur vers le nœud source.

L'exactitude des messages RSVPv2 n'est pas vérifiée parce que cela est seulement nécessaire dans des environnements où plusieurs implémentations de RSVP ont à interagir. En effet, dans RSVPv2/NS, les messages RSVPv2 sont toujours traités par le même processus RSVPv2 qui a généré les messages.

C- La classe RSVPv2agent

Pour une session donnée, les structures utilisées à l'intérieur des agents RSVPv2 sont les suivantes :

- *RSB (Resv State Blocks)* : chaque RSB maintient l'état du *Resvv2* pour une requête de réservation correspondant au n-tuplet (SESSION2, SENDER_TEMPLATE2, FILTER_SPEC2, STYLE2, FLOWSPEC2, SENDER_TSPEC2, RECEIVER_TEMPLATE2, MAP_TEMPLATE2, RESV_CONFIRMv2, RSVP_HOP2).

  Le contenu du RSB comprend les attributs suivants provenant du message RESVv2 :

  - TTL IP restant ;
  - l'adresse IP du hop précédent à partir de l'objet PHOP ;
  - l'interface logique LIH (Logical Interface Handle) à partir de l'objet PHOP ;
  - l'interface logique OI (Outgoing Interface) sur laquelle la réservation doit être faite ou a été faite.

- *TCSB (traffic control state block)*: Chaque TCSB maintient la spécification de la réservation qui a été faite pour le contrôle du trafic pour une interface sortante spécifique. En général, l'information du TSCB est obtenue à partir de celle du RSB pour la même interface OI. Chaque TSCB définit une

réservation unique pour un n-tuple particulier : (SESSION2, OI, FILTER_SPEC2).

- *Session* : Pour chaque session à l'intérieur d'un agent RSVPv2, il existe une structure *session*. Cette structure contient différents champs, incluant un pointeur vers la liste de RSBs (rsb_list) avec tous les états importants du *resvv2* pour cette session et un pointeur vers la liste de TCSBs (tcsb_list). Il contient également une étiquette *confirm*, qui détermine si un objet RESV_CONFIRMv2 sera transmis avec le prochain message *Resvv2* pour demander un accusé de réception (ou de confirmation) de la réservation (pour les sessions sur les nœuds de terminaux).

Les attributs majeurs de la classe *RSVPv2agent* sont :

- *s_list* : liste contenant toutes les sessions avec leurs *RSBs* et leurs *TCSBs* (Figure a.2) ;
- *t_list* : liste des temps (*timers*) qui est utilisée afin de planifier les sessions pour l'envoi de messages de rafraîchissement (*refresh*).

Pour chaque état *Resvv2* d'une session à la Figure a.2, une structure *rsb* est ajoutée à la liste RSB de la session, il comprend différents objets et un pointeur vers l'objet *RSVPv2Checker*.

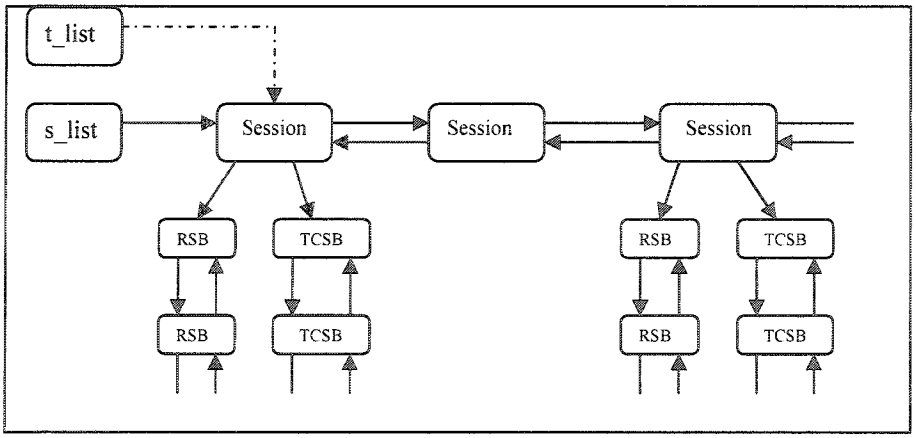


Figure a.2 Liste de *session* et de *timer*

Cet objet se charge de transmettre le message RSVPv2 à l'agent qui a entraîné la création du RSB. Le champ *timeout* conserve le moment à partir duquel l'état *resvv2* va expirer, à moins qu'il soit rafraîchi par des messages *Resvv2*. Dans le TCSB pour une session donnée, les réservations actuelles pour chaque lien sortant sont conservées.

Les agents RSVPv2 maintiennent l'état des réservations sur tous les nœuds RSVPv2, génèrent des messages RSVPv2 et traitent les messages RSVPv2 entrant. Les méthodes de la classe *RSVPv2agent* les plus importantes sont les suivantes :

- *new_session_sid* : cette méthode crée une nouvelle session, l'ajoute à la liste de sessions et retourne l'identificateur de la dite session créée ;
- *new_session_p* : elle crée une nouvelle session, l'ajoute à la liste de sessions et retourne un pointeur vers la session ;
- *new_rsb* : cette fonction crée un nouveau RSB pour une session donnée et l'ajoute à la liste de RSB ;
- *update_rsb* : cette méthode permet de mettre à jour un PSB existant avec de nouvelles valeurs ;
- *refresh* : elle rafraîchit l'état des réservations pour toutes les sessions qui ont besoin d'être rafraîchie ;
- *check_resv* : cette fonction vérifie si un état Resvv2 est terminé et devrait être retiré. Elle retourne 1 si la session a été retirée pendant le traitement, autrement elle retourne 0 ;
- *send_resv_message* : elle crée et envoie un message Resvv2 pour un PSB dans une session. De même, nous avons *send_resv_tear_message*, *send_resv_err_message* et *send_resv_conf_message* pour l'envoi respectif des messages *ResvTearv2*, *ResvErrv2* et *Ackv2*.
- *update_traffic_control* : elle permet de trouver tous les RSBs qui correspondent au triplet (session, émetteur, prochain_hop) pour le RSB actif,

de déterminer le *LUB* de leurs spécifications de flots (FLOWSPECS) puis de faire une requête de contrôle d'admission et d'effectuer une réservation si possible ;

- *process_resv_message* : cette fonction permet à l'agent RSVPv2 d'effectuer le traitement d'un message Resvv2 à un nœud. Pour le traitement respectif des messages *ResvTearv2*, *ResvErrv2* et *Ackv2*, nous avons également les autres méthodes *process_resv_tear_message*, *process_resv_err_message* et *process_resv_conf_message* ;
- *find_rsb* : cette fonction trouve un RSB pour une session dont l'adresse donnée SENDER_TEMPLATE2 et le FILTER_SPEC2 sont équivalents à l'adresse de l'émetteur. Elle retourne NULL si aucun RSB n'est trouvé ;
- *find_session_sid* : elle retourne un pointeur vers la session ayant l'identificateur de session *sid* ou retourne NULL si rien n'est trouvé ;
- *find_session_dst* : elle retourne un pointeur vers la session ayant l'adresse de destination *dst* et l'identificateur de flot *fid* ou retourne NULL si rien n'est trouvé.

a.3 Résultat et analyse complémentaires

a.3.1 Le délai de bout en bout d'un paquet

Les Figures a.3 et a.4 présentent le délai de bout en bout d'un paquet en fonction respectivement du routage triangulaire et du routage optimal pour le scénario Fast FH-RSVP Straight. Dans les deux cas étudiés, le nœud mobile se déplace à une vitesse v de 5 m/s et les paquets CBR UDP de 200 octets sont transmis à un débit de 64 kbps. De façon générale, nous pouvons observer à la Figure a.3 et à la Figure a.4 que le MN réussit à maintenir un délai de bout en bout d'un paquet stable d'environ 109 ms pour le routage triangulaire (pire cas) et d'environ 59 ms pour le routage optimal (meilleur cas) lors de la simulation. Nous remarquons que les résultats obtenus concordent avec les

estimations théoriques des équations (3.10) et (3.11) faites au chapitre 3. Le délai d'un paquet est relativement constant avec FH-RSVP pour les mêmes raisons évoquées pour le débit.

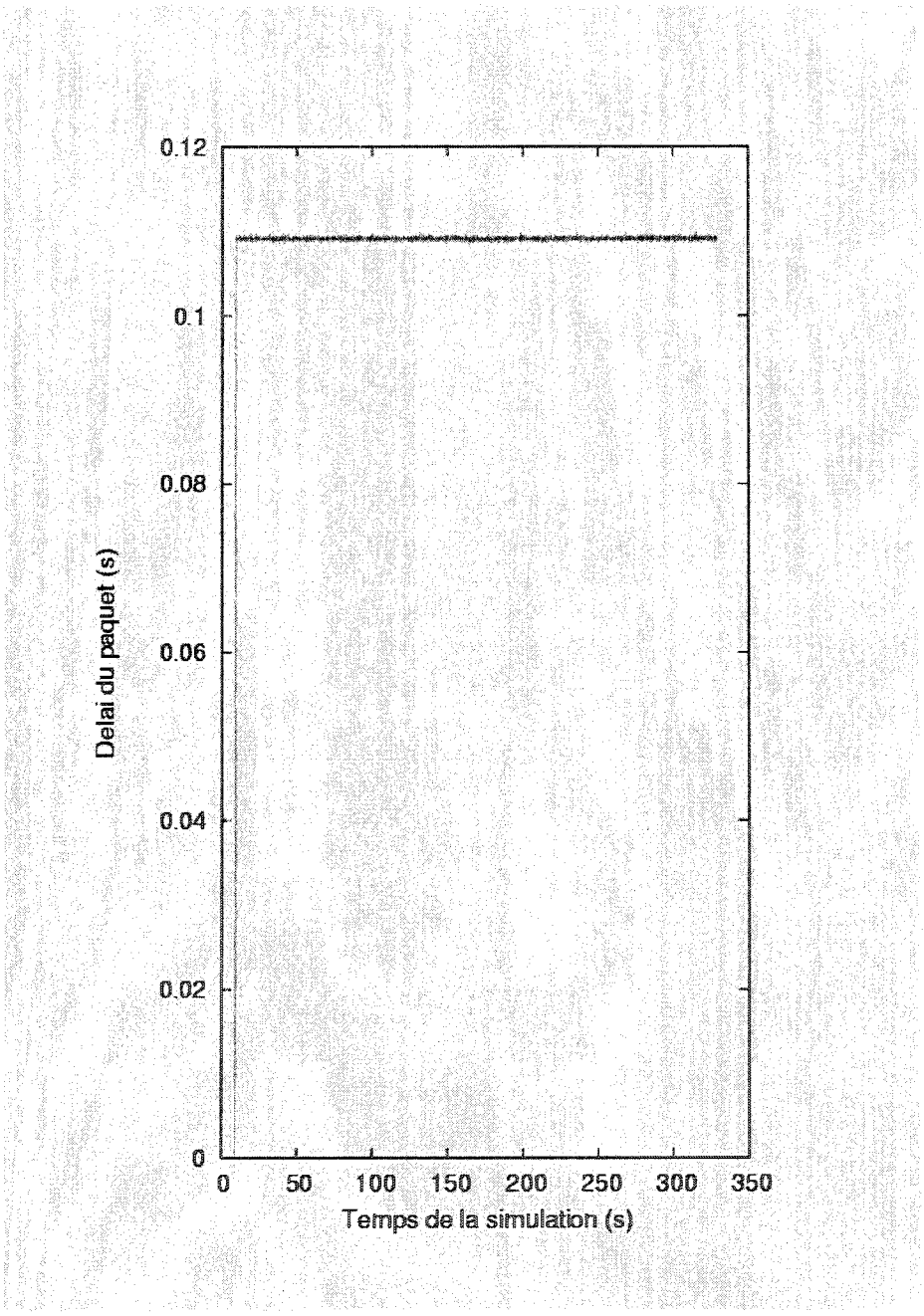


Figure a.3 Délai d'un paquet – Fast FH-RSVP – routage triangulaire

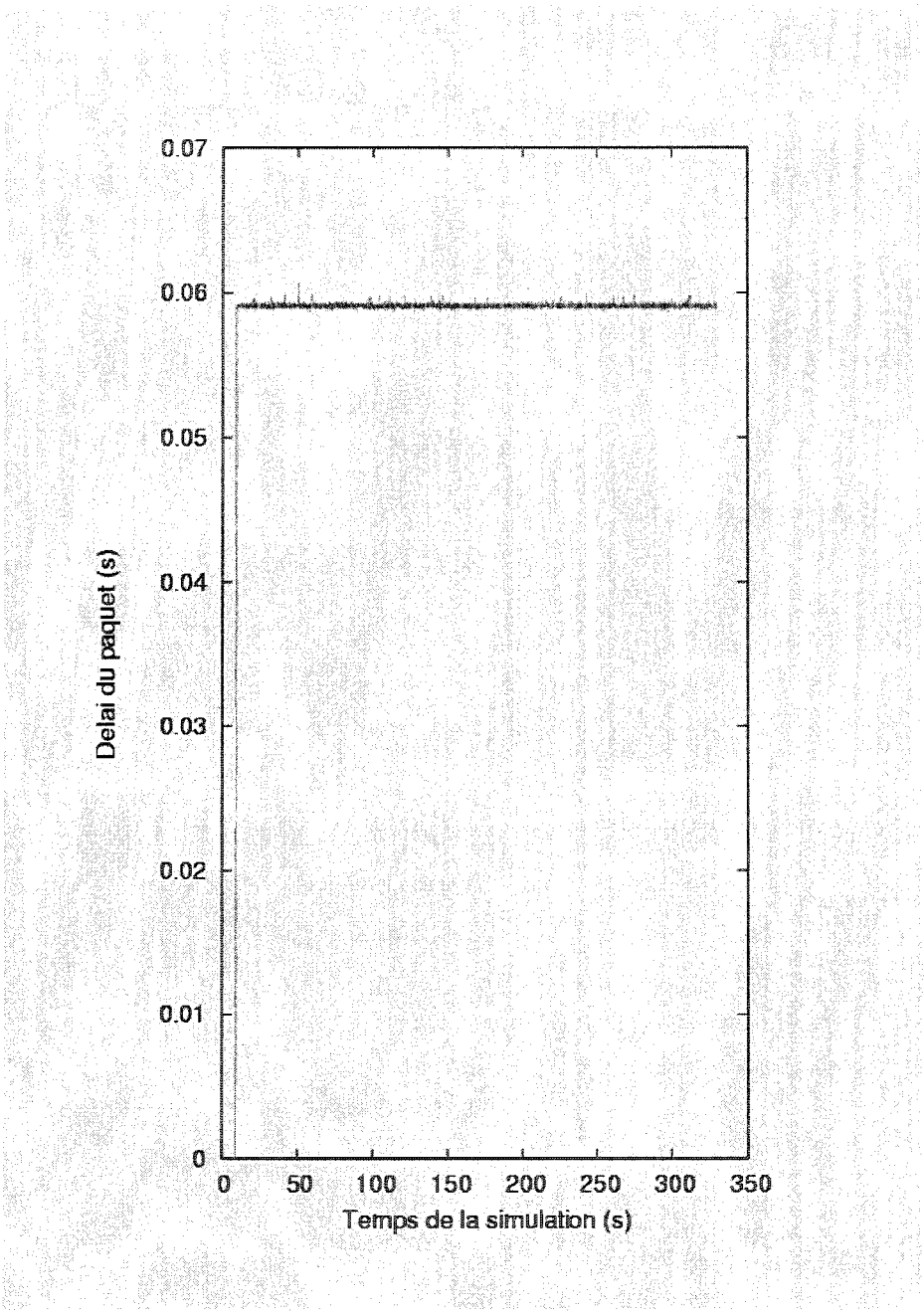


Figure a.4 Délai d'un paquet – Fast FH-RSVP – routage optimal